TokenWeaver: Privacy Preserving and Post-Compromise Secure Attestation

Cas Cremers[1], Charlie Jacomme[2], and Eyal Ronen[3]

[1]CISPA Helmholtz Center for Information Security, Germany
[2]Inria Paris, France
[3]Computer Science Department, Tel Aviv University, Tel Aviv, Israel

December 5, 2022 – v1.0

Abstract

Modern attestation based on Trusted Execution Environments (TEEs) can significantly reduce the risk of secret compromise by attackers, while allowing users to authenticate across various services. However, this has also made TEEs a high-value attack target, driving an arms race between novel compromise attacks and continuous TEEs updates.

Ideally, we would like to ensure that we achieve Post-Compromise Security (PCS): even after a compromise, we can update the TEE into a secure state. However, at the same time, we would like the privacy of users to be respected, preventing providers (such as Intel, Google, or Samsung) or services from tracking users.

In this work, we develop TokenWeaver, the first privacy-preserving post-compromise secure attestation method with automated formal proofs for its core properties. We base our construction on weaving together two types of token chains, one of which is linkable and the other is unlinkable. We provide the full formal models, including protocol, security properties, and proofs for reproducibility, as well as a proof-of-concept implementation in python that shows the simplicity and applicability of our solution.

1 Introduction

One of the most basic requirements for secure communication is the ability to authenticate the identity of remote parties. Proving one's identity usually involves proving the knowledge of some secret, such as a password or cryptographic key. However, the security of any authentication scheme is only as strong as the security of the secrets used for authentication. If an attacker is able to compromise the device that stores the secrets and extracts them, it can exploit them for impersonation. To mitigate such attacks, a Trusted Execution Environment (TEE) such as ARM's TrustZone [2], AMD's Secure Encrypted Virtualization (SEV) [25], and Intel's SGX [14] offers a secure and isolated environment at the hardware level that can be used to protect sensitive secrets. Remote attestation allows a device to prove that it is running the latest and most secure software version and that cryptographic keys were generated and used inside a TEE.

In practice, remote attestation introduces two additional requirements. First, we would like to protect users' privacy: no one should be able to track users as they access different services by exploiting the remote attestation mechanism, which can be expressed as an unlinkability property. For example, if Alice uses her device for remote attestation to two different third-party servers, they shouldn't be able to learn it is the same device or even if they both collude with the provider.

Second, we would like to achieve Post-Compromise Security (PCS) [13]. In the past few years, we have seen a large number of attacks that are able to extract cryptographic keys and bypass the attestation of even state-of-the-art TEEs such as TrustZone [37, 38, 41, 48], SEV [8, 28–30, 35, 46, 47], and SGX [5, 10, 16, 19, 21, 26, 27, 31, 36, 40, 42–45]. Although subsequent software or microcode patches usually mitigate the attacks, all previous secrets stored in the TEE might have been compromised. This raises the natural question of how to recover the trust in our attestation process even when cryptographic keys are leaked, i.e., whether we can achieve PCS.

Unfortunately, standard mechanisms for PCS seem at odds with unlinkability. Intuitively, achieving PCS requires to "track" the usage of secrets: even if it is possible to revoke certificates regularly, which is one

of the mechanisms we will rely on, a provider then needs to know it is only delivering new valid certificates to uncompromised TEEs, and for instance not to a clone. However, privacy requires unlinkability, i.e., to prevent any "tracking" of the usage of secrets. Due to the importance of this problem, both Google and Intel attempted to solve it (for TrustZone and SGX, respectively), but as we will show, only partial solutions were given. Thus, we ask ourselves the following question:

Is it possible to maintain and recover security while still preserving the privacy of users?

Contributions

In this paper, we provide TokenWeaver, the first formal-analysis co-design solution for a privacy-preserving and post-compromise secure attestation with TEEs. To achieve this, we proceed in the following steps:

- We define and model the concrete security goals and requirements for a privacy-preserving and PCS secure remote attestation.
- We design both linkable and unlinkable one-time provably secure privacy-preserving and PCS authorization mechanisms.
- We leverage these mechanisms to build the fully-fledged TokenWeaver solution that a TEE provider can use to provision tokens that support both anonymous and non-anonymous attestation to third-party parties while achieving both PCS and privacy-preserving w.r.t to third parties and the TEE provider.
- Unlike existing solutions, we formally model and prove the core properties of TokenWeaver and provide reproducible results at [15]. Notably, our co-design allowed us to detect and fix an early design flaw.
- To advocate for the simplicity and applicability of our solution, we provide a python-based proof-of-concept.

Outline

We describe background and related work on remote attestation in the TEE setting, and the main security requirements in Sections 2 and 3. We define the core building blocks for our solution in Section 4, and present our complete solution in Section 5. We formally analyze the security of our solution in Section 6, and describe our proof-of-concept implementation in Section 7. We discuss limitations and future work in Section 8 and conclude in Section 9.

2 Background

We first describe what we mean by Remote Attestation in the TEEs setting and what the functional goals are. We then informally describe the security goals, and finally describe the existing solutions and their limitations.

2.1 Remote attestation in the TEE setting

Context description

The scenario we are considering involves the following parties:

- A trusted provider (e.g., Intel, Google, or Samsung);
- A user;
- A user device with a TEE set up by the provider; and
- A set of third-parties that the user interacts with through its device.

Each TEE is set up by the trusted provider. Such TEEs should be able to run a small and sensitive code base securely and in isolation from the "Normal World" (that includes the operating system and regular applications). Additionally, they should be able to *attest* that they are valid TEEs to third parties, either using an Anonymous Certificate (AC) or using a Non Anonymous Certificate (NAC). ACs are used to attest to being *some* valid TEE, and NACs are used to attest to being a *specific* valid TEE with a Serial Number (SN). This attestation capability is the core functionality that we wish to design in this work. As such, the main functionalities that need to be considered from the TEE point of view are:

1. Attestation to a third party;
2. Provisioning of new certificates from the provider;

Point 1) is the core usage case of TEEs, and Point 2) is essentially the certificate provisioning and management. To ensure some security guarantees, additional mechanism are then added to those functionalities

Requirement

From a high-level point of view, we assume the following requirement to realize remote attestation. The provider owns a master key pair, whose public key is globally trusted. The provider sets up each individual TEE environment (e.g., an enclave) with a unique SN and a unique secret (or set of secrets). These allow to establish a secure and authenticated channel between the TEE and the provider. Additionally, the TEE can store and use certificates for attestation to third-parties that can either be anonymous or linked to the specific SN of the TEE. These certificates only certify that they are owned by a valid and up-to-date TEE. Note that the certificates are provisioned by the provider and can be updated periodically (e.g., once a month) or on demand (e.g., as part of a pushed software update). The TEE's firmware may itself be updated. Furthermore, the TEE has a verified boot feature, which can authenticate the firmware it is running.

2.2 Informal Security goals

A first basic security goal of the certificate provisioning is **Authentication**: only valid TEEs can successfully obtain certificates from the provider.

In this paper, the more advanced property we aim to achieve deals with the possibility of compromise, namely **Post-Compromise Security (PCS)**. In many security protocols, compromising the state of some honest agent implies a complete security loss (at least in regard to that agent). However, for protocols that have a state-update mechanism, PCS specifies that it is possible to recover from compromise: after a compromise of some honest agent's state, if the honest agent performs one more step of the protocol, the honest agent should be able to **heal**, and the attacker can be locked out again. In the context of TEEs, PCS can be formulated in multiple equivalent ways:

- If the attacker compromised a TEE that healed afterwards, the attacker cannot obtain certificates anymore;
- Conversely, the only way for the attacker to obtain valid certificates is to compromise a device that did not heal afterwards.

For a full compromise, this property has a side effect: if the attacker can use the compromised state to perform a healing update before the honest party does, the honest user will be locked out, since the provider cannot distinguish between the honest party and the attacker that compromised *all* data. This leads us to two additional desirable properties:

- **Clone Detection**: if a user is locked out due to an attacker compromise, this is detected and the user will be notified.
- **Active revocation**: if the clone detection mechanism is triggered, we require an independent mechanism that allows to completely reset the protocol, locking out the attacker and restoring the trust for the honest user. Active revocation typically needs to rely on some out-of-band channel to restore the state of the protocol.

Finally, we want to achieve PCS but in a **privacy-preserving** way. For example, if the provider and several third-party servers collude, they might be able to track the usage of certain certificates across multiple servers, and even link them to a specific device or group of devices. From the provider's point of view, we expect that the provider is never able to tell that a particular TEE performed an action or not (anonymity), and whether some actions were performed by the same TEE or not (unlinkability) even when colluding with third-party servers.

2.3 Existing solutions and limitations

Google

Google's certificate provisioning for Android is defined through their APIs, and some informal descriptions of the internal details are available [20]. Roughly speaking, Android Attestation aims to achieve PCS, and a recent version update explicitly claimed this goal. Android Attestation will keep a list of known-compromised software and will not allow devices running this version to be provisioned (although it is not clear what properties of PCS they claim to achieve). However, if we were to analyze only the user-facing API, it would appear that it would be possible for Google to track users using this mechanism. The

informal description [20] states that tracking is prevented by a so-called *split-brain* solution: internally, Google strictly separates the verification of the device's public key from the processing of the attestation key. If done correctly, this means the server that verifies the device key (and thus knows which device) never learns the attestation keys that are handled by other servers, preventing the attestation keys from being linked to the device key. However, this cannot be externally verified, and depends on Google enforcing this policy internally through some additional mechanism.

SGX

Intel provides a method for remote attestation for code running inside the SGX enclave based on Enhanced Privacy ID (EPID) [7]. It extends the previous Direct Anonymous Attestation (DAA) solution [6] with enhanced revocation capabilities. The code running inside the enclave is signed using an Intel-provisioned private key. The signature is then verified by Intel's Attestation Server (IAS). At a technical level, EPID uses bilinear pairing to support anonymous attestation. It also supports revocation by requiring clients to prove that they did not generate previous signatures that were flagged (using a zero-knowledge proof of discrete logarithm inequality). Note that the cost of verification grows linearly with the number of revoked signatures, so in practice, only a small number of revocations can be supported. It provides PCS by updating the EPID keys using dedicated shared symmetric keys called the "Provisioning Key". However, it is not clear how PCS can be achieved if the symmetric long-term secret is compromised. Recently, Intel proposed a new ECDSA-based attestation called SGX DCAP [39] that does not provide anonymity.

Limitations

Existing solutions are lacking in two respects:

- the recovery mechanisms only work against a weak attacker; and
- privacy concerns are at best addressed informally.

Indeed, Google's solution only offers privacy as long as one trusts Google, which is a surprising setting for privacy. Further, it does not offer explicit recovery mechanisms: they claim recovery is possible, but specify no way of detecting compromise. Intel's solutions are expensive through the use of EPID, and PCS is only provided assuming a partial compromise of the TEE. As such, we propose in the next sections a treatment of possible **privacy preserving and post-compromise secure attestation mechanisms for TEEs.**

2.4 Further related work

More generally, our work can be seen as neighbor to the anonymous credentials research area. In this context, we previously mentioned how Direct Anonymous Attestation [6] was in fact the ancestor of EPID.

Recently, Privacy-pass [17] was proposed to provide an anonymous user-authentication mechanism. They use a Verifiable Oblivious Pseudo-Random Function (VOPRF) to provision anonymous tokens, that can for instance be used to reduce the number of CAPTCHAs challenges specific users are requested to solve. Our work can also be linked to the anonymous blacklisting/whitelisting ideas from [22]: intuitively, only the set of honest TEE can obtain certificates.

In general, none of these works match our specific needs. While such techniques could be reused to emulate the blinded token part in the unlinkable chain, for instance with a VOPRF, they would not allow for delivering blindly signed certificates that the TEE can then use to third parties. Since we already rely on blind signatures for the third-party functionality, we chose to also use them for the blinded tokens. And of course, more crucially, none of the proposals provide or even consider PCS.

3 Concrete Security Goals

We previously presented the high level PCS and privacy goals. In this section, we discuss more precisely what the concrete security goals are in the TEE setting and for which attackers, notably with respect to the potential compromise.

Compromise Threat Model

Our goal is to consider strong attackers that can compromise the TEE in multiple ways, and classify when and how it is possible to recover from or detect a compromise. Concretely, we consider two levels of compromise:

- Compromised certificates, or
- Compromise of the long-term secrets.

Distinguishing these two levels make sense as the long-term secrets are stored more securely and used only for a dedicated set of operations, while the certificates can be accessed (and misused) through the API by multiple applications as was exploited in [41].

Each of those compromise implies different level of possible PCS guarantees. In this work, we will try to obtain the best possible guarantees, either locking out or detecting the attacker after different level of compromises. We will formally express the PCS properties we obtain in Section 6, and notably systematize which guarantees we obtain for which compromise in Section 6.5.

3.1 Privacy and Recovery limitations

We next discuss some high-level limitations of the design space based on distinct types of compromise: full and persistent compromise; full and non-persistent compromise, and certificate compromise.

Full and persistent compromise

In the case of full and persistent compromise, anonymous attestation is a difficult property to guarantee. Indeed, a basic observation is that it is enough for only a single TEE to be compromised so that we can no longer trust any anonymous attestation. Here, there are two layers to consider. If the compromise is a full compromise at the API level, the attacker can perfectly emulate the TEE to anybody, including providers and third parties. As such, not only is anonymous attestation no longer secure, but any recovery mechanism will fail as it is impossible to distinguish an honest TEE from the attacker. In such a full compromise of a TEE, only a physical recall of the devices (to deliver a tamper-proof firmware upgrade) might allow for recovery.

Full and non-persistent compromise

In the case of a full but non-persistent compromise, the attacker can perfectly emulate the honest TEE, but at some point, the honest TEE may try to contact the provider again. Here, it may be possible that the provider can detect the clone and the honest user should receive a warning in this scenario. An inherent limitation here is that the provider cannot tell who is the clone and who is the honest user. To recover from this state, we require some out-of-band connection that can be established between the user and the provider.

A difficulty is that in such cases, revoking only some certificates is useless as the attacker can simply obtain new ones from the provider by emulating the honest TEE. This highlights the need for other recovery mechanisms to either **lock-out** or **detect** the attacker, as we design with TokenWeaver.

Certificate compromise

The compromise of the certificates only is the simplest sort of compromise, that can be caused e.g., by a faulty firmware version where the API can be abused, or through some hardware extraction [41].

A natural solution is then to revoke the compromised certificates, which can be anonymous or non-anonymous (and provision new ones). There are multiple flavors of **revocation** depending on who wants to revoke what and when:

- **Provider targeted** the provider revokes a targeted user certificates;
- **Firmware update** the provider revokes all certificates corresponding to a known vulnerable version of the firmware;
- **User triggered** a user revoke his own certificates;
- **Time based** all certificates regularly expire.

The first and third approach have drawbacks in terms of privacy: in the first one the provider must already be able to target the certificate of a compromised users, which are then not anonymous, and in the third case the user may reveal its identity or link previous attestations in order to have its certificates revoked. A user may however wish to trigger a full reset after going through a border control for instance, even at the cost of losing some privacy. The second and fourth solution both appears like good practice and do not appear to have direct privacy consequences.

Privacy against Providers and Third-parties

As we previously mentioned, there is inherent tension between the privacy requirement and the clone detection requirement, which restricts the possible design choices.

To express the multiple flavors of privacy one may expect in an anonymous attestation case, let us denote by $Update^{X}_{AC}$ the action where the provider provisioned a new AC to a given TEE X and Use^{x}_{AC} the use of the of some AC by the TEE to attest something to a third-party. Informally, the anonymity tells us that from the point of view of the provider, we should have $Update^{A}_{AC} \approx Update^{B}_{AC}$, that is, a provisioning performed by the TEE A is indistinguishable from one by B. But we actually need a stronger property if we consider that the provider and third-parties collude, which is that $Update^{A}_{AC}.Use^{B}_{AC} \approx Update^{B}_{AC}.Use^{B}_{AC}$, that is, it is impossible to link a given certificate provisioning from a given attestation step. And finally, we expect that $Update^{A}_{AC}.Update^{A}_{AC} \approx Update^{B}_{AC}.Update^{C}_{AC}$, that is, the provider cannot link together multiple updates of the same device.

This last unlinkability requirement leads to an interesting problem. How can the provider detect a clone if it cannot tell if two updates originated from the same device or two different devices?

To resolve this apparent contradiction, the core idea is that while the provider should not know whether two updates link back to the same device, the provider can make sure that the same update from the same state is never performed twice. However, this seems to lead to a strong performance implication, a new update needs to prove that it is an update that was never done before, with respect to all previous updates of all TEEs. We remark that classical mechanisms such as counters for clone detection trivially fail to satisfy the privacy requirements, as observed for instance by the WebAuthn specification [32, Section 6.1.1].

4 Authorization Chains for PCS

In this section, we describe the two core mechanisms that we will use for the certificate provisioning:

- a **linkable authorization token chain**, which will gives us PCS in a simple way, but will not provide any privacy;
- a **unlinkable authorization token chain**, which will give us both PCS and privacy by relying on so-called blind signatures.[1]

We first present those two mechanisms independently from the TEE context, as they are generic mechanisms for the following question: *how to perform a recurring authorization from a client to a server with PCS and privacy?* The context is then that we have a server S, and a set of authorized clients C. We assume that C can easily establish a one-sided authenticated channels to S, for instance using TLS. Then, each client C should be able to confirm it is one of the authorized clients, and may have to perform this operation regularly. In the TEE context, the clients will be the TEEs and the server the provider. The security goals will be similar to those in Section 2.2, namely authentication, PCS and unlinkability.

4.1 Linkable Authorization Token Chain

The simplest way to establish an authorization mechanism would be to deliver to each client an authentication key pair $\mathsf{pk}_C, \mathsf{sk}_C$ that each authorized client uses to authenticate to the server. However, after a client compromise, the attacker would obtain the corresponding secrets, enabling the attacker to keep logging in indefinitely.

To design an authorization mechanism that achieves PCS, one possibility is to have the server deliver one-time authorization tokens to clients. Clients should present a valid one-time tokens to perform a single authorization step, and every time the authorization is successful, the server delivers a freshly generated authorization token to the client. This first mechanism requires that the server maintains a set $\mathsf{ValidTok}$ of currently valid authorization tokens. Then, the following steps are followed:

- Whenever a new client is registered for the first time, the server generates a fresh token, and adds it to $\mathsf{ValidTok}$ and provides it to the client.
- To perform an authorization, a client with current token t establishes a TLS connection with the server and sends t over the connection.

[1] Note that as is done in [17], Verifiable Oblivious Pseudo-Random Function (VOPRF) can be used instead of blind signatures. However, as the full TokenWeaver solution requires the provisioning of anonymous certificates for third-party servers, we use blind signatures that can be used for both use cases.

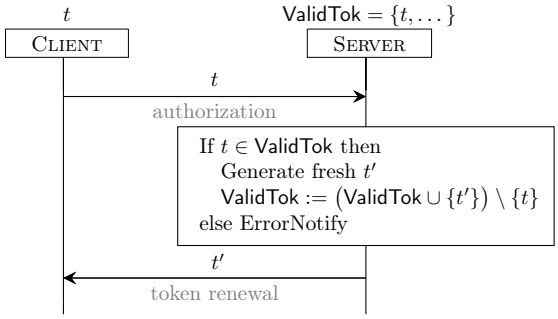

Figure 1: Linkable Authorization Token Chain

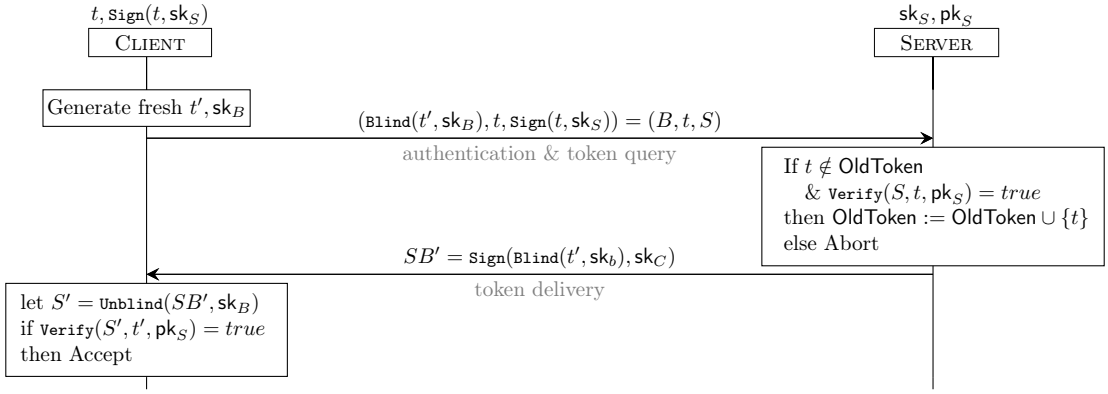

Figure 2: Unlinkable Authorization Token Chain

- The server then verifies that the token is valid, i.e. $t \in \mathsf{ValidTok}$, in which case the authorization succeeds. The server then generates a new fresh token t', removes t and adds t' to $\mathsf{ValidTok}$, and finally sends t' back to the client.

We show this simple flow in Fig. 1.

Security Intuition

The crucial observation is that each token can be used only once, and cannot be predicted. When a client is compromised, the attacker learns the current t. However, once the client performs a subsequent authorization, t is consumed on the server side, and the attacker is effectively locked-out again.

However, this design offers no strong privacy. In fact, each client is linkable by the server: the server can effectively remember the previous token delivered to some client, and then recognize that a new connection comes from the same client when this specific token is presented. This allows reconstructing the full chain of tokens corresponding to a given client.

4.2 Unlinkable Authorization Token Chain

We now consider a client C that wishes to perform the authorization process in a completely unlinkable way while retaining PCS. The core issue in the previous mechanism is that the server knows each authorization token owned by the clients. Our solution is then to make it so that the tokens are not generated by the server but rather by the client. The server will not even learn the token but will only *blindly* sign it with a dedicated signing key. This blind signature can later be verified to check the token validity.

Blind signatures

We use so-called blind signature schemes [9]. Such a signature scheme is defined by four algorithms $(\mathtt{Sign}, \mathtt{Verify}, \mathtt{Blind}, \mathtt{Unblind})$, such that for a valid keypair $(\mathsf{sk}_S, \mathsf{pk}_S)$, $(\mathtt{Sign}, \mathtt{Verify})$ is a classical signature scheme, but with the additional feature that for a freshly sampled blinding key sk_b, $\mathtt{Blind}(m, \mathsf{sk}_b)$ reveals no information about m, and even a *malicious server* cannot link $\mathtt{Blind}(m, \mathsf{sk}_b)$ and the unblinded signature $\mathtt{Sign}(m\, \mathsf{sk}_s)$, and of course $\mathtt{Unblind}(\mathtt{Sign}(\mathtt{Blind}(m, \mathsf{sk}_b), \mathsf{sk}_s), \mathsf{sk}_b) = \mathtt{Sign}(m\, \mathsf{sk}_s)$.

Setup

We consider that the server S has a signature key pair $(\mathsf{sk}_S, \mathsf{pk}_S)$, and the client C already has a token t (a nonce) along with a proof of validity of the token $\texttt{Sign}(t, \mathsf{sk}_S)$. S maintains a set of expired tokens $\mathsf{OldToken}$, initialized with the empty set.

Process description

Assume that C can establish an authenticated channel to S (e.g. via a TLS certificate for S). Then, the authentication and token renewal process is depicted in Fig. 2.

1. C generates a blinding key sk_b and a new secret token t', and send the values $\texttt{Blind}(t', \mathsf{sk}_B), t, \texttt{Sign}(t, \mathsf{sk}_S)$ to S.
2. S receives B, t, S, checks the validity of the given token by running $\texttt{Verify}(S, t, \mathsf{pk}_S)$ and checking that $t \notin \mathsf{OldToken}$. If so, authentication succeeds, the server deprecates the token by updating $\mathsf{OldToken} := \mathsf{OldToken} \cup \{t\}$, and sends $\texttt{Sign}(\texttt{Blind}(t', \mathsf{sk}_b), \mathsf{sk}_C)$ to the client. If the token was already used, the server notifies the user that it owns a deprecated token.
3. C computes $\texttt{Unblind}(\texttt{Sign}(\texttt{Blind}(t', \mathsf{sk}_b), \mathsf{sk}_S), \mathsf{sk}_b) = S'$, runs $\texttt{Verify}(S', t', \mathsf{pk}_S)$ and if it is valid, it stores the token t' along with its signature S'.

Security Intuition

Intuitively, our solution meets the expected security properties.

- **Authentication**: The unforgeability of the signature ensures that only people with a valid token can obtain a new token.
- **Privacy**: Thanks to the blinding, the server does not know which token it is delivering to which client. Note that it is *crucial* that the client does check it got a valid signature, as otherwise the server could maliciously deliver a broken signature to detect the later use of this particular token. This check was actually missing from our initial protocol draft, but the flaw and the attack were discovered automatically by our tools when we tried to formally prove it.
- **PCS**: If a client is compromised and the token is stolen, either the client first uses it and the token obtained by the attacker becomes useless, or if the attacker first uses it and then the client tries to use it, the update will fail and the compromise will be detected.

Crucially, we note that the detection of the compromise in this initial design has a significant limitation. If the attacker did use the honest user's token, the honest user update will fail and they could report it to the server. However, even if the compromise is detected, the server can only deliver a new token to the honest user, but it *cannot deprecate* the attacker's token, as due to the blind signatures and the resulting unlinkability, the server has no information about this token. We are thus missing the active revocation capability. In the next section, we show how to solve this remaining issue.

5 TokenWeaver

We now define our full solution, dubbed TokenWeaver, that combines the previously presented linkable and unlinkable token chains in order to achieve the full certificate provisioning solution. The only cryptographic dependency is on classical and blind signature schemes. The TEE uses the unlinkable chain between itself and the provider for on-demand provisioning of new certificates for third-party authentication. This ensures quick recovery from compromise as well as privacy. On top of it, a linkable chain between the provider and the TEE allows to reset the linkable chain in case the attacker locked out the honest user, adding support for revocation. We provide in the following all the protocols comprising TokenWeaver and in Fig. 3 a summary of the high-level states machines of the multiple entities. We additionally provide in Appendix A a full specification in pseudo-code.

In the descriptions, we assume that we can establish a unilaterally authenticated channel to the Provider, where only the Provider is authenticated, in order to send a single message and receive a single answer such that messages are confidential and integrity protected. Such a channel can easily be built, for instance by relying on existing TLS certificates of the Provider. We provide additional details on how to define, build, and use this channel in Appendix B.

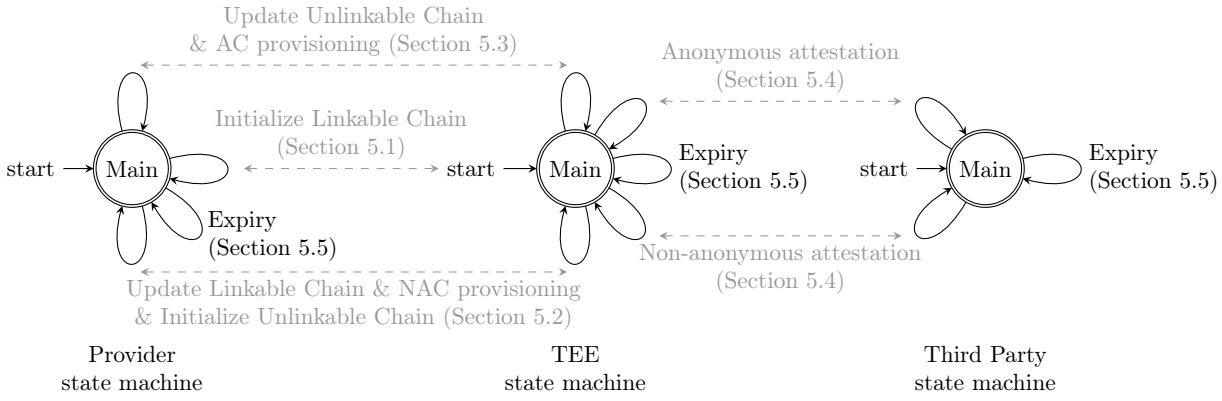

Figure 3: TokenWeaver: high-level state machines and connecting protocols indicated with dashed edges. The Provider and the TEEs states evolves together either when 1) a new TEE is created (initialization of the linkable chain), 2) a TEE perform a linkable chain update or 3) a TEE perform an unlinkable chain update. A TEE and a third party state evolve when a TEE performs a (non)-anonymous attestation. The only operation where all agents are updated is upon the global provider certificate expiry.

Cryptographic materials

To ease the presentation of the underlying protocols, we now highlight all materials owned by either the provider or the TEEs and their use, for a summary see Table 1 in Appendix A. We first consider that the provider owns two distinct key pairs:

- **attestation key pair** $\mathsf{sk}_A, \mathsf{pk}_A$: this is the public key trusted by third parties for the attestation aspect.
- **provisioning key pair** $\mathsf{sk}_P, \mathsf{pk}_P$: this is the key pair used by the provider for signing tokens in the unlinkable authorization chain.

Both key pairs should expire and be renewed frequently to ensure that attackers are eventually locked out. The expiration of sk_P and sk_A is our only way of locking out an attacker that compromised some unlinkable token.

The state of a TEE then depends on the following values:

- A SN - a public identifier of the TEE.
- Current valid AC and NAC - multiple TEE owned key pairs signed by the current sk_A, that can be used to attest to third parties. AC is fully anonymous, while NAC is tied to the SN. They are implicitly deprecated when sk_A is renewed.
- A current unlinkable one-time authorization token $t, \mathtt{Sign}(t, \mathsf{sk}_P)$ - when presented to the provider, the token is consumed. In return, the TEE can generate a new token t' and ask the provider to blindly sign it with sk_P. In addition, the provider also blindly signs a new key pair for AC generated by the TEE using the latest sk_A.
- A linkable one-time authorization token t_l - This token is used to renew the unlinkable one-time authorization token (e.g., when sk_P is renewed). When t_l is presented to the provider, it is consumed, the provider delivers a new token t'_l, and blindly signs a new token t' generated by the TEE. The provider also signs a new NAC key-pair with sk_A.

The full states of the multiple parties can be summarized as in Fig. 4. In practice, t_l is used less often and should be better protected if possible in concrete deployments.

5.1 TEE initialization

Instantiating a new TEE is straightforward as it only requires to initialize the linkable token chain. Note that to be fully functional and obtain valid certificates, the TEE will then need to perform an linkable chain update followed by an unlinkable chain update as described in the following.

Setup

At the factory, the provider generates and provides a fresh token t_l to the TEE identified by SN, and stores the pair (t_l, SN) inside the set $\mathsf{LinkedToken}$.

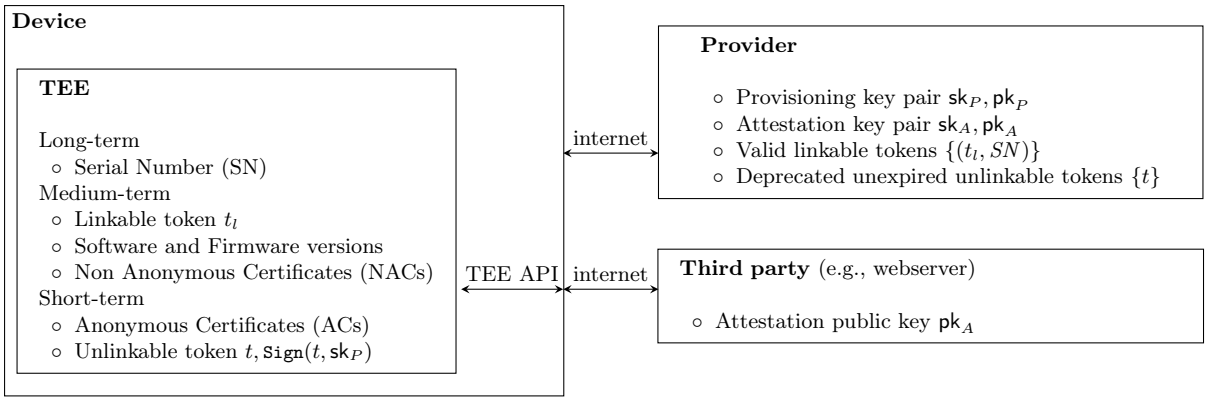

Figure 4: TokenWeaver's TEE setup

5.2 Update Linkable Chain

We describe here the full update of a linkable chain, which leverages the mechanism from Section 4.1 to initializes or re-initializes the TEE's unlinkable chain and additionally delivers a new NAC. This step must be performed every time sk_P is deprecated.

Protocol description

To (re-)initialize the unlinkable chain and receive a new NAC the following steps are followed:

- the TEE establishes a one-way authenticated encrypted channel to the provider (e.g., a TLS channel based on the provider's PKI certificate);
- the TEE generates a new secret token t', a blinding key sk_b, and a fresh key pair $\mathsf{sk}_{NAC}, \mathsf{pk}_{NAC}$. He then sends the values $\texttt{Blind}(t', \mathsf{sk}_B), t_l, \mathsf{pk}_{NAC}$ to the provider.
- the provider checks that there exists SN such that $(t_l, SN) \in \mathsf{LinkedToken}$, in which case it drops it from the list, generates a fresh t'_l, adds (t'_l, SN) to $\mathsf{LinkedToken}$, and then sends back the values $\texttt{Sign}(\texttt{Blind}(t', \mathsf{sk}_b), \mathsf{sk}_P), t'_l, \texttt{Sign}((SN, \mathsf{pk}_{NAC}), \mathsf{sk}_A)$.
- the TEE computes

$$\texttt{Unblind}(\texttt{Sign}(\texttt{Blind}(t', \mathsf{sk}_b), \mathsf{sk}_O), \mathsf{sk}_b) = S' \ ,$$

  and runs $\texttt{Verify}(S', t', \mathsf{pk}_P)$. If the verification is successful, it stores t'_l as its new linkable token, (t', S') as its current unlinkable token, and $(\mathsf{pk}_{NAC}, \mathsf{sk}_{NAC}, \texttt{Sign}((SN, \mathsf{pk}_{NAC}), \mathsf{sk}_A)$ as its NAC.

If at any time a honest user is locked out because an attacker already used the token t_l, the honest user must use some out-of-band authentication and send a compromise report to the provider containing its SN. In this case, the provider erases any entry linked to SN inside $\mathsf{LinkedToken}$, thus deprecating the current linkable token actually used by the attacker, and then should communicate a fresh t_l to the TEE through a secure out-of-band communication channel to the user.

Note that if a TEE updates its linkable chain multiple times in the lifespan of a single sk_P, it would obtain multiple valid blinded tokens and be able to initiate multiple parallel unlinkable chains. However, they would all still be deprecated simultaneously when the corresponding sk_P expires.

5.3 Update Unlinkable Chain

We now leverage the unlinkable chain mechanism from Section 4.2 to perform the AC provisioning. We assume here that the TEE has a valid unlinkable token $t, \texttt{Sign}(t, \mathsf{sk}_P)$ for the current provisioning key of the provider. Otherwise, it must first run the previous mechanism.

To achieve anonymous attestation, we run the AC provisioning in parallel to the unlinkable chain update. The TEE generate their own attestation key pairs and ask the provider to blindly sign it with the latest sk_A, which yields an AC. As this process can be run multiple times, the TEE can accumulate multiple distinct ACs. Using a different AC for attestation to each third-party server (or each account) preserves the unlinkability of the attestation process.

Protocol description

The AC provisioning is performed in parallel to a valid unlinkable chain update as follows:

- At any time, a TEE may choose to generate a new attestation key pair $\mathsf{sk}_T, \mathsf{pk}_T$. It then establishes a secure session with the provider (e.g., over TLS with a certificate for the provider), and then performs a one-time authorization, including the authorization the value $\texttt{Blind}(\mathsf{pk}_T, \mathsf{sk}'_b)$ (with sk'_b a fresh blinding key) in the first message.
- The provider processes the one-time authorization, and if it is valid, includes in its answer $BSA' = \texttt{Sign}(\texttt{Blind}(\mathsf{pk}_T, \mathsf{sk}'_b), \mathsf{sk}_A)$.
- The TEE processes the answer and stores the new token. It additionally stores $SA' = \texttt{Unblind}(BSA', \mathsf{sk}'_b)$, after successfully verifying that SA' is a valid signature.

Every time a TEE runs such a process, it has:

- A valid one-time anonymous authentication token $(t, \texttt{Sign}(t, \mathsf{sk}_S)$ from completing the one-time unlinkable authorization process;
- A new attestation key pair $\mathsf{sk}_T, \mathsf{pk}_T$ along with a valid certificate of the public key $\texttt{Sign}(\mathsf{pk}_T, \mathsf{sk}_A)$.

Due to the blind signature, the provider learns no information about the attestation key pair that it provided a certificate for. Furthermore, the TEE can now attest itself to any third party by using sk_T to sign a challenge and send the signature and the certificate $\texttt{Sign}(\mathsf{pk}_T, \mathsf{sk}_A)$.

5.4 Attestation: Certificate Verification

Assuming that a TEE is up to date and has performed a full AC provisioning valid for the current attestation public key pk_A, it should currently own:

- at least two signing secret keys, sk_T and sk_{NAC};
- at least two certificates, a non anonymous one $\texttt{Sign}((SN, \mathsf{pk}_{NAC}), \mathsf{sk}_A)$ and an anonymous one $\texttt{Sign}(\mathsf{pk}_T, \mathsf{sk}_A)$.

Such a TEE can then use either sk_T or sk_{NAC} to sign any desired data, and send this signature along with the corresponding certificate to a third party. The third party then simply has to validate the certificate chain, verifying the validity of the current public attestation key of the provider pk_A.

A TEE can perform multiple AC provisioning to obtain additional signing keys sk_T. When attesting to service so that the TEE should be unlinkable, a distinct AC must then be used.

Security Intuition

We provide a formal analysis in Section 6, but on an intuitive level, we inherit the PCS guarantees from the one-time authorization token. However, the concrete privacy we achieve depends on the implementation details of the third party attestation process. Our scheme prevents the provider and third party servers from linking together a particular TEE with any of its ACs or linking together different ACs used by the same TEE. However, in some use cases, the attestation process itself may leak some metadata that can be exploited to link together distinct attestations even when using different ACs (e.g., the device's IP address). As this is application dependent, we consider it to be outside the scope of our work.

5.5 Expiring public keys

The provider needs to manage the renewal of the two public keys pk_A and pk_P. The expiration should be time-based to ensure PCS. Here, any classical technique used to manage public keys can be plugged in, in a similar fashion to TLS certificate management. For example, a third longer term key could be published by the provider and used to sign the two sub keys along with the expiry date.

6 Formal Analysis

In this section, we describe in-depth the formal analysis of the core elements of TokenWeaver, providing stronger assurance guarantees than any other solution in this domain. The analysis was performed in parallel to the design, its results allowing us to update the design whenever an issue was reported. Our ideal proof goals are ambitious: a complete coverage of all the goals of the full design is currently beyond the reach of any single automated analysis tool. To obtain our strong guarantees, we therefore use a combination of state-of-the-art protocol verification tools.

In particular, we perform three distinct analyses:

- We first prove that in isolation, the unlinkable token chain is indeed unlinkable.

- We then show that the unlinkable token chain in isolation does meet the expected PCS property. We also illustrate how the formal analysis reported an attack on a previous design, and lead us to improve it.
- Finally, for the full AC provisioning mechanism, including both linkable and unlinkable chains, we prove that the linkable chain does meet PCS, and that linkable chain does lock out an attacker from the unlinkable chains.

We were not able to study the unlinkability of the full solution due to limitations of the tools, as the complexity of the models lead to non-termination.

Reproducibility

All automated formal analyses carried out in this section where performed on a laptop with 16Gb of RAM and a quad-core Intel(R) Core(TM) i7-10510U CPU at 1.80GHz and can easily be inspected or reproduced. We provide the models at [15] along with instructions to download a docker image allowing readers to inspect and reproduce the analyses and proofs.

6.1 Choosing appropriate proof tools

The main mechanisms of our solution occur at the logical level: TokenWeaver can be seen as a complex stateful security protocol that keeps several different layers of state, but also depends on cryptographic primitives. This combination suggests that state-of-the-art symbolic protocol analysis tools may be appropriate, such as Tamarin [34] or Proverif, which can provide proofs for unboundedly many sessions. Because of the type of state machines in the protocol, and because we expected the complexity to be beyond the scope of fully automated proofs, we chose Tamarin.

However, during our analysis, it became clear that while Tamarin was appropriate for proving PCS, neither Tamarin nor Proverif currently provide for the privacy properties we wanted to prove for TokenWeaver. While Tamarin and other tools allow to verify a specific class of privacy properties, they only support proving a property that is too strong for our situation: for those tools, updating the state of one TEE and not another one lead to a false attack. As we require a fine grained notion of privacy, we thus turn to the DeepSec prover [11]: it has the downside of forcing us to consider only a fixed number of TEEs and possible updates, but it can verify a privacy notion that is fine-grained enough for our situation.

Thus, using this combination of tools, we can prove PCS properties for a complex model with an unbounded of TEEs and updates, and also fine-grained privacy properties for a fixed number.

6.2 Privacy Analysis of the Unlinkable Chain

To analyze the privacy properties, we use DeepSec, which can verify that two scenarios are indistinguishable by the attacker. We describe now the two scenarios we compared. In this section, we only provide a high level intuition without formally defining the underlying security properties. We provide further details in Appendix C.

Our DeepSec model

We model two TEEs that, after initialization, can both perform unlinkable and linkable updates. After performing a linkable update, a TEE state should contain a valid unlinkable token pair $(t, \mathtt{Sign}(t, \mathsf{sk}_P)$. We then model the fact that it can make a one step authorization, where it authenticates to the provider using t and renew its unlinkable token obtaining a new valid t' as well as obtaining a new AC.

We consider a threat model where the attacker controls all external elements to the TEE. Crucially, we thus consider that the Provider is malicious and attacker-controlled.

Note that whenever a TEEs did not perform the latest linkable update after sk_P expired, it does not have a valid token. It is then easy to distinguish an unlinkable update from a TEE that did the latest linkable update compared to one that did not. We therefore aim to prove that when two TEEs have both made the same number of linkable updates, then a scenario where only a single TEE performs unlinkable updates is indistinguishable from the scenario where the two different TEEs are performing updates.

Using DeepSec, we verified that this property holds, which corresponds to proving that an attacker can not tell if two updates are linked, whenever the two TEEs are both either up to date or outdated with respect to sk_P.

As mentioned, DeepSec only works for a bounded number of protocol sessions, and the proof complexity increases exponentially with respect to the number of sessions. We can prove the unlinkability

for 16 total updates (8 linkable and 8 unlinkable ones) in under a minute. Despite the exponential growth, we can push the numbers by using a server with more RAM and parallelization. On a 64 cores CPU at 2.60GHz and with 23Gb of RAM, we were able to go up to 24 total updates (12 linkable updates and 12 unlinkable updates), verified in about 20 hours.

Our formal analysis caught an early design error

An early version of our design did not include verification of the resulting blind signature by the TEE in the last step of the unlinkable chain update. When we tried to prove the unlinkability of this version with DeepSec, we uncovered a simple attack on the design that DeepSec reported in under a second. Without verification, a malicious provider can return an invalid signature. This can be exploited later on to track the TEE, as the provider can spot when it receives an invalid signature, thus violating unlinkability. We subsequently updated our design.

6.3 PCS Analysis of the Unlinkable Chain

We used Tamarin to carry out the analysis that proves the unlinkable chain provides PCS against an attacker that can compromise the tokens of the chain.

Model

We modeled the core unlinkable mechanism as described in Fig. 2. Our model covers an unbounded number of TEEs (client) interacting with the provider (server), and contains the following possible actions:

- **Initialize** - Initialization of a new TEE, which sends a blinded token to the provider and receives the corresponding signature. We assume the communication is done over a trusted channel where the provider can authenticate the TEE, e.g., initialization done at the factory.
- **TEE Query** - A TEE sends its current token as well as a fresh blinded one to the Provider over a secure channel.
- **Provider Answer** - The provider checks the validity of the token, deprecates it, and returned the blind signature on the new one.
- **TEE Process** - The TEE checks the validity of the provided signature, and stores the new token.

There are two possible attacker actions:

- **Compromise** - The attacker can compromise a given TEE and obtain its current token.
- **Attacker Query** - The attacker can contact the provider and try to perform a step of the process with any message it can compute based on its knowledge.

Property

To model security properties such as authentication of PCS, we rely on so called events: whenever a possible action is executed, we add to the execution trace the corresponding event. We can then express security properties over those events inside a temporal logic.

For instance, in our models, we raise the event $\mathsf{Accept}(t)$ whenever the provider accepts a token t, $\mathsf{Query}(t)$ when a TEE sends the token t in the query step. For a TEE, processing a new token corresponding to healing, so we raise $\mathsf{Heal}(SN)$ whenever a TEE identified by SN performs the TEE process action and should then have healed, and $\mathsf{Compromise}(SN)$ whenever the attacker compromises the TEE corresponding to SN. Then, the PCS property can intuitively be expressed as follows: If a provider accepts a token at timepoint i then:

- either there exists a TEE that sent it as a query at a previous timepoint $j < i$;
- or the attacker compromised a TEE at a previous timepoint $j < i$, and between i and j the TEE never healed.

This property essentially captures the only possible ways for a token to be accepted. The first case corresponds to a valid token processing, and the second one to an attacker token processing. Note that if the attacker compromise a TEE that heal afterward, then only honest token processing can happen, and the attacker is locked out and cannot interfere with the process anymore. Formally, it then translates to:

$$\begin{aligned} &\forall\, t, i.\ \mathsf{Accept}(t)@i \Rightarrow \\ &\quad (\exists\, j.\ \mathsf{Query}(t)@j \ \&\ j < i) \\ &\quad \| \left(\begin{array}{l} \exists\, SN, j.\ \mathsf{Compromise}(SN)@j \ \&\ j < i \\ \quad \&\ \neg(\exists\, k.\ \mathsf{Heal}(SN)@k \ \&\ j < k \ \&\ k < i \end{array} \right) \end{aligned}$$

Proof

To prove such a property, Tamarin works in a so called backward fashion: for our PCS property, it starts from the Accept state, and will try to prove that all possible ways to get to a state that violates the property are impossible. As we consider an unbounded number of updates, the problem is in general undecidable. Tamarin then relies on heuristics to choose an optimal next proof rule out of its set of possible proof rules. In our case, Tamarin's built-in heuristics are not able to automatically find a proof. However, Tamarin has an interactive proof mode, which we can use to guide the proof search, either by adding helper lemmas, or by performing ourselves the proof in the interactive mode.

To carry out this proof, the core difficulty is to show that if the provider accepts a token sent by the attacker, but that the compromised TEE healed, then there is a contradiction (i.e., such a state cannot be reached). The issue is that the token sent by the attacker may be the i-th token sent by it since the compromise, and that the heal of the TEE may also be the j-th healed performed by the TEE since its compromise. We then have to go back in the past, showing that if this i-th attacker token is valid, and this j-th token is valid, the there exists a $i-1$ attacker token and a $j-1$ TEE heal. By reasoning inductively, we will then finally reach a state where the attacker must have used the first token it obtained, the one from the compromised, and the TEE healed using the same token. This leads to a contradiction as this particular compromised token can only be processed once by the provider.

We formalized such lemmas in Tamarin, and were able to prove the PCS property with a total of 9 lemmas, 6 of them automatically proven by Tamarin and 3 proven by hand for a total of 174 proof steps. Tamarin verifies the corresponding proof files in under 10 seconds.

6.4 PCS Analysis of the AC provisioning

Model

We model the two linkable and unlinkable chains in Tamarin intertwined as described in Section 5. The model specifies the following possible actions:

- **Renew keys** - renew the provider keys sk_P and sk_A.
- **Initialize** - create a fresh TEE instantiated with a valid linkable token.
- **Linkable chain query** - a TEE establishes a secure channels and sends its current linkable token along with a blinded token and a fresh blinded public key pk_T;
- **Linkable chain answer** - the provider checks the validity of the linkable token, in which case it signs the blinded token with the current sk_P and the blinded pk_T, and send it along with a new fresh linkable token.
- **Linkable chain process** - the TEE receives and stores its new linkable and unlinkable tokens after unblinding and verifying the received signatures.
- **Unlinkable chain Query/Answer/Process** - the three possible actions from the previous model (Section 6.3) are then possible, where as long as the TEE as an unlinkable token signed with the current sk_P, it can then obtain a new AC certificate signed with the current sk_A.

The attacker can **Compromise** a TEE, in which case it gets the linkable and unlinkable tokens that it can use to obtain valid certificates for the compromised TEE. The attacker can also send its own unlinkable or linkable queries to the provider and obtain valid certificates for its own TEEs.

Properties

We have previously proved that each unlinkable chain gives us PCS. When combined with the linkable chain, we have to prove that:

- the linkable chain itself provides PCS: if the attacker compromise a linkable token, it can either use it and lock the user out, or the user will use it and the attacker is locked out.
- renewing the keys of the provider then ensure the global PCS: after a key is renewed, the only way for the attacker to continue obtaining ACs is to use a linkable token it compromised.

The first property is similar to the previous one for the unlinkable case. We can in fact be slightly more precise, as the provider knows which TEE it is authenticating. We now raise the event $\mathsf{AcceptL}(t, SN)$ whenever the provider accepts a linkable token t corresponding to TEE SN, $\mathsf{QueryL}(t, SN)$ when the TEE sends the token t in the query step, and $\mathsf{HealL}(SN)$ whenever the TEE finishes the final linkable process action and should then be healed. We still raise $\mathsf{Compromise}(SN)$ whenever the attacker compromise the TEE corresponding to SN, where the compromise is common to both the linkable and unlinkable

processes.

$$\begin{aligned}\forall\, t, SN, i.\ \mathsf{AcceptL}(t, SN)@i \Rightarrow \\ (\exists\, j.\ \mathsf{Query}(t, SN)@j\ \&\ j < i) \\ \|\ \left(\begin{array}{l}\exists\, j.\ \mathsf{Compromise}(SN)@j\ \&\ j < i \\ \quad \&\ \neg(\exists\, k.\ \mathsf{HealL}(SN)@k\ \&\ j < k\ \&\ k < i\end{array}\right)\end{aligned}$$

We can show that if the attacker compromises a TEE and then the keys are renewed, the attacker needs to use the linkable token it obtained to keep getting new ACs. The only way for the attacker to keep compromising the system is thus to lock out the honest user, which enables clone detection. If we raise the event Renew whenever the provider keys are renewed, raise the event AcceptUAtt when the attack succeed in performing an unlinkable authorization, and raise the event AcceptLAtt when it succeeds in performing a linkable authorization, we can then formally express the property as:

$$\begin{aligned}\forall\, i, j, k.\ \mathsf{Compromise}(SN)@i\ \&\ \mathsf{Renew}@j\ \& \\ \mathsf{AcceptUAtt}@k\ \&\ i < j < k \\ \Rightarrow \exists\, l.\ \mathsf{AcceptLAtt}@l\ \&\ j < l < k\end{aligned}$$

This property precisely expresses that if a compromise happened at a timepoint i and the keys were renewed afterwards at $j > i$, then if the attacker can still perform an unlinkable step later at $k > j$, it must have in fact performed a linkable step at timepoint l in between j and k. The converse of this property then tells us that if the attacker did not perform the linkable step, it is locked out of the AC provisioning.

Proofs

The intuition of the proof is close to the previous one. On the one hand it is simpler, because there is no cryptography involved inside the linkable process, but on the other hand it is more complex, because the full model is bigger. Overall, we needed 19 lemmas, 2 of them being the target properties, 13 of them proved automatically and 6 of them proved manually in 425 steps. The full model verifies in about 15 seconds.

Encoding assumptions

An implicit assumption in our Tamarin analysis is that the encodings of NAC $\mathtt{Sign}((SN, \mathsf{pk}_{NAC}), \mathsf{sk}_A)$ and AC $\mathtt{Sign}(\mathsf{pk}_{AC}, \mathsf{sk}_A)$ are disjoint. The underlying reason is that in the natural symbolic encoding of public keys, a pk_{AC} can never be equal to a pair of elements (SN, pk_{NAC}). In most implementation, this separation is naturally achieved by the formatting and encoding of public keys and tuples. For implementations that do not ensure this separation, one could either include a label or also use two distinct keys instead of a single sk_A to achieve domain separation.

6.5 Summary of provable security guarantees

Based on our formal analysis, we can summarize the security guarantees of our solution as follows.

Privacy

We proved that the unlinkable chain combined with the linkable chain and the AC provisioning ensures unlinkability. There are cases not covered by our analysis that include naturally unavoidable breaches of privacy:

- when a TEE uses a NAC; or
- when a TEE reuses the same AC for two distinct use cases, or use an AC while leaking non-anonymous metadata.

It would be interesting to be able to express a fine-grained unlinkability property over the full system, additionally capturing those behaviors and metadata. It would also be interesting to lift the limitation on the bound on the number of sessions. Both of those points however appear to require further advances in formal methods development.

PCS with compromise of unlinkable token or certificate

This is the most likely compromise, as the unlinkable token and the certificates are used frequently. In this case, our PCS proof of the unlinkable chain shows that if the honest user uses the unlinkable token, the attacker cannot obtain any new certificates. Additionally, the certificates obtained by the attacker

will expire when the provider renews the attestation key sk_A. If the attacker first uses its clone of the unlinkable token, the user will detect it when trying to use it. Then, the user could renew its certificate using the linkable token and reveal its compromised NAC to the provider. The provider could then, e.g., publish it in a deprecated certificate list.

PCS with compromise of linkable token

This is a deeper compromise, as the linkable token is only used to reset the unlinkable chain. In this case, our PCS proof of the linkable token chain shows that if the user uses the linkable token, it locks the attacker out of the linkable chain. The attacker can still run the unlinkable certificate provisioning as long as the provider keys are not renewed. However, our analysis of the AC provisioning shows that as soon as the provider's keys expire, the only way the attacker can keep getting valid certificates is by running the linkable update. If an attacker does so, it would lock the user out and would be detected. In such a case, the user sends a compromise report to the provider, who deprecates any linkable token corresponding to this user's TEE. Then, the provider can use a secure out-of-band channel to provide a fresh linkable token to the TEE.

7 Proof of Concept Implementation

To advocate for the simplicity and applicability of our solution, we implemented in python the operations described in Section 5 for the full AC provisioning. Our un-optimized proof of concept is available at [15]. Our goal is not to perform fine-grained time-measurements that would rely on the particularities of specific use-case details, but to show the simplicity of our generic core design. The solution takes 41 lines of code for the TEE, 28 for the provider side, and 8 lines for the Third-Party. The core cryptographic dependency is a blind signature scheme, for which we use the reference implementation of the under-standardization RSA-BSSA proposal [18] proved secure in [33]. For the actual attestation, an extra signature is required, for which we use a standard RSA signature scheme. A linkable token update round requires one blind signature and verification and an additional standard signature for the NAC, An attestation requires one standard signature from the TEE. On the third party side, it requires one blind signature verification and one standard signature verification. Due to the low number of asymmetric cryptographic operations and keys on the client side, we argue that the complexity of our provisioning protocol is equivalent to other widely deployed cryptographic protocols such as TLS, FIDO, and EPID. Because such cryptographic primitives and protocols are commonly implemented and used inside modern TEEs, we claim that our protocol is efficient and practical for this application domain.

In terms of space, the provider needs to maintain a list containing a pair (t_l, SN) for each TEE, as well as a list containing all the deprecated unexpired unlinkable tokens, list which is reset whenever the public key pk_P expires.

8 Discussions

Global Attestation Key Variant

In this work we presented a solution where each TEE can obtain a set of multiple ACs, and a single AC should be dedicated to a single use case, as otherwise colluding third party could link multiple attestation to the same TEE. This has the downside of requiring that each TEE manages and keeps track of which account is linked to each AC, and of having the TEE request potentially many ACs to the provider.

To enable a fully anonymous attestation, the simplest solution is for the provider to just give sk_A to all TEEs, and each TEE simply use this secret key to perform attestation. This ensures the privacy as all TEEs share the same attestation key.

In practice, we need to frequently renew the keys to enable for recovery. We thus tie this idea with the one-time authentication mechanism, where every time the provider renew the keypair, all TEEs perform an authorization upon which the provider sends them the new secret key. We thus consider the case where the provider owns a keypair $\mathsf{sk}_A, \mathsf{pk}_A$ for attestation, and a keypair $\mathsf{sk}_S, \mathsf{pk}_S$ for the authorization part. Then:

- All TEEs are initialized at the factory with a token $t, \mathtt{Sign}(t, \mathsf{sk}_S)$.
- Regularly the provider renew the key pair $\mathsf{sk}_A, \mathsf{pk}_A$.
- When a TEEs requires a new valid key sk_A, it first establish a TLS connection with the provider, and then performs a one-time authorization to the provider as depicted in Fig. 2.

- Whenever the provider accepts a valid token, it additional appends to its reply the value sk_A.

While simpler than TokenWeaver, the global key does not allow to instantly revoke the current ACs of a TEE when a user detects a compromise. Further, our solution also allows to detect or recover from compromises earlier, as it implies more frequent interactions between the TEE and the provider.

Mitigation of DoS Attack

Malicious devices might attempt a Denial-of-Service (DoS) attack by repeatedly requesting new tokens. However, as we show in Section 7, the computational cost of such a request is relatively low (similar to the cost of a TLS handshake), making it less useful for DoS attacks. Moreover, the provider can add a rate-limiting mechanism for token provisioning. It can insert a time delay between the time a token is provided and when it can be used to request a new one.

Linkable token

For the linkable token t_l, the provider is required to store for each TEE a pair (t_l, SN). Other solutions could be considered, e.g., counters, or chains based on repeated application of a pseudo-random function, combined with zero-knowledge proofs. We leave exploring alternative solutions based on such mechanisms as future work.

Third-Party Authorization

A third-party can decide to set up their own Authorization Token process with a TEE (which is independent from the one with the provider). The mechanism can for instance be used by a third-party to provide one-time tokens to access a resource in a privacy preserving way, and in parallel ask for an attestation from the TEE.

Version-linked tokens

Tokens could be linked to the firmware, to allow to deprecate all tokens corresponding to some outdated insecure firmware. This would however be redundant with the recurrent expiration of sk_A.

9 Conclusions

We presented TokenWeaver, a solution for privacy-preserving and post-compromise secure attestation. TokenWeaver is based on a combination of both linkable and unlinkable token chains, which may be of independent interest.

Compared to Google's split brain solution, we obtain true privacy, and do not have to trust the provider to uphold an internal split. This is a crucial distinction, since (a) users cannot verify that the split brain policy is actually implemented, and (b) even if implemented, the split may be breached over time. Compared to SGX, we have no need for EPID. Notably, SGX makes no claims (let alone proofs) of PCS.

In contrast to both of these solutions, we offer *provable* PCS and privacy properties. Additionally, we offer fine-grained clone detection, both at the linkable and unlinkable levels.

References

[1] Myrto Arapinis, Tom Chothia, Eike Ritter, and Mark Ryan. Analysing unlinkability and anonymity using the applied pi calculus. In *2010 23rd IEEE computer security foundations symposium*, pages 107–121. IEEE, 2010.

[2] Arm. Arm TrustZone technology. https://developer.arm.com/ip-products/security-ip/trustzone.

[3] David Baelde, Stéphanie Delaune, and Solène Moreau. A method for proving unlinkability of stateful protocols. In *2020 IEEE 33rd Computer Security Foundations Symposium (CSF)*, pages 169–183. IEEE, 2020.

[4] David Basin, Saa Radomirovic, and Michael Schläepfer. A complete characterization of secure human-server communication. In *2015 IEEE 28th Computer Security Foundations Symposium*, pages 199–213. IEEE, 2015.

[5] Pietro Borrello, Andreas Kogler, Martin Schwarzl, Moritz Lipp, Daniel Gruss, and Michael Schwarz. ÆPIC Leak: Architecturally Leaking Uninitialized Data from the Microarchitecture. In *USENIX Security*, 2022.

[6] Ernest F. Brickell, Jan Camenisch, and Liqun Chen. Direct anonymous attestation. In *CCS*, pages 132–145. ACM, 2004.

[7] Ernie Brickell and Jiangtao Li. Enhanced privacy ID: A direct anonymous attestation scheme with enhanced revocation capabilities. *IEEE Transactions on Dependable and Secure Computing*, 9(3):345–360, 2011.

[8] Robert Buhren, Hans-Niklas Jacob, Thilo Krachenfels, and Jean-Pierre Seifert. One glitch to rule them all: Fault injection attacks against AMD's secure encrypted virtualization. In *CCS*, pages 2875–2889, 2021.

[9] David Chaum. Blind signatures for untraceable payments. In *CRYPTO*, 1983.

[10] Guoxing Chen, Sanchuan Chen, Yuan Xiao, Yinqian Zhang, Zhiqiang Lin, and Ten H Lai. SgxPectre Attacks: Stealing Intel Secrets from SGX Enclaves via Speculative Execution. In *EuroS&P*, 2019.

[11] Vincent Cheval, Steve Kremer, and Itsaka Rakotonirina. DEEPSEC: deciding equivalence properties in security protocols theory and practice. In *2018 IEEE Symposium on Security and Privacy (SP)*, pages 529–546. IEEE, 2018.

[12] Vincent Cheval, Steve Kremer, and Itsaka Rakotonirina. Exploiting symmetries when proving equivalence properties for security protocols. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, pages 905–922, 2019.

[13] Katriel Cohn-Gordon, Cas Cremers, and Luke Garratt. Post-Compromise Security. Cryptology ePrint Archive, Paper 2016/221, 2016. https://eprint.iacr.org/2016/221.

[14] Victor Costan and Srinivas Devadas. Intel SGX Explained. Cryptology ePrint Archive, Paper 2016/086, 2016. https://eprint.iacr.org/2016/086.

[15] Cas Cremers, Charlie Jacomme, and Eyal Ronen. Formal models for the Tamarin prover and DeepSec and Proof of Concept Python implementation of TokenWeaver, Dec 2022. https://github.com/charlie-j/token-weaver.

[16] Fergus Dall, Gabrielle De Micheli, Thomas Eisenbarth, Daniel Genkin, Nadia Heninger, Ahmad Moghimi, and Yuval Yarom. CacheQuote: Efficiently recovering long-term secrets of SGX EPID via cache attacks. *CHES*, 2018.

[17] Alex Davidson, Ian Goldberg, Nick Sullivan, George Tankersley, and Filippo Valsorda. Privacy pass: Bypassing internet challenges anonymously. *Proc. Priv. Enhancing Technol.*, 2018(3):164–180, 2018.

[18] Frank Denis, Frederic Jacobs, and Christopher A. Wood. RSA Blind Signatures. Internet-Draft draft-irtf-cfrg-rsa-blind-signatures-04, Internet Engineering Task Force, August 2022. Work in Progress.

[19] Dmitry Evtyushkin, Ryan Riley, Nael CSE Abu-Ghazaleh, ECE, and Dmitry Ponomarev. BranchScope: A New Side-Channel Attack on Directional Branch Predictor. In *ASPLOS*, 2018.

[20] Max Bires Google Android developers blog. Upgrading Android Attestation: Remote Provisioning, March 2022. https://android-developers.googleblog.com/2022/03/upgrading-android-attestation-remote.html (Accessed 10 August 2022).

[21] Jago Gyselinck, Jo Van Bulck, Frank Piessens, and Raoul Strackx. Off-limits: Abusing legacy x86 memory segmentation to spy on enclaved execution. In *ESSoS*, 2018.

[22] Ryan Henry and Ian Goldberg. Formalizing anonymous blacklisting systems. In *2011 IEEE Symposium on Security and Privacy*, pages 81–95. IEEE, 2011.

[23] Lucca Hirschi, David Baelde, and Stéphanie Delaune. A method for verifying privacy-type properties: the unbounded case. In *2016 IEEE Symposium on Security and Privacy (SP)*, pages 564–581. IEEE, 2016.

[24] ISO 15408-2: Common criteria for information technology security evaluation - part 2: Security functional components, July 2009.

[25] David Kaplan, Jeremy Powell, and Tom Woller. AMD memory encryption. *White paper*, 2016.

[26] Zijo Kenjar, Tommaso Frassetto, David Gens, Michael Franz, and Ahmad-Reza Sadeghi. V0LTpwn: Attacking x86 Processor Integrity from Software. In *USENIX Security Symposium*, 2020.

[27] Esmaeil Mohammadian Koruyeh, Khaled Khasawneh, Chengyu Song, and Nael Abu-Ghazaleh. Spectre Returns! Speculation Attacks using the Return Stack Buffer. In *WOOT*, 2018.

[28] Mengyuan Li, Yinqian Zhang, and Zhiqiang Lin. CrossLine: Breaking "security-by-crash" based memory isolation in AMD SEV. In *CCS*, pages 2937–2950, 2021.

[29] Mengyuan Li, Yinqian Zhang, Huibo Wang, Kang Li, and Yueqiang Cheng. CipherLeaks: Breaking constant-time cryptography on AMD SEV via the ciphertext side channel. In *USENIX Security*, pages 717–732, 2021.

[30] Mengyuan Li, Yinqian Zhang, Huibo Wang, Kang Li, and Yueqiang Cheng. TLB poisoning attacks on AMD secure encrypted virtualization. In *ACSAC*, pages 609–619, 2021.

[31] Moritz Lipp, Andreas Kogler, David Oswald, Michael Schwarz, Catherine Easdon, Claudio Canella, and Daniel Gruss. PLATYPUS: Software-based Power Side-Channel Attacks on x86. In *IEEE S&P*, 2021.

[32] Emil Lundberg, Akshay Kumar, J.C. Jones, Jeff Hodges, and Michael Jones. Web authentication: An API for accessing public key credentials - level 2. W3C recommendation, W3C, April 2021. https://www.w3.org/TR/2021/REC-webauthn-2-20210408/.

[33] Anna Lysyanskaya. Security analysis of RSA-BSSA. *Cryptology ePrint Archive*, 2022.

[34] Simon Meier, Benedikt Schmidt, Cas Cremers, and David Basin. The TAMARIN prover for the symbolic analysis of security protocols. In *International conference on Computer Aided Verification (CAV)*, pages 696–701. Springer, 2013.

[35] Mathias Morbitzer, Manuel Huber, Julian Horsch, and Sascha Wessel. Severed: Subverting AMD's virtual machine encryption. In *EuroSec*, pages 1–6, 2018.

[36] Kit Murdock, David Oswald, Flavio D. Garcia, Jo Van Bulck, Daniel Gruss, and Frank Piessens. Plundervolt: Software-based Fault Injection Attacks against Intel SGX. In *IEEE S&P*, 2020.

[37] Pengfei Qiu, Dongsheng Wang, Yongqiang Lyu, and Gang Qu. VoltJockey: Breaching TrustZone by software-controlled voltage manipulation over multi-core frequencies. In *CCS*, pages 195–209, 2019.

[38] Keegan Ryan. Hardware-backed heist: Extracting ECDSA keys from Qualcomm's TrustZone. In *CCS*, pages 181–194, 2019.

[39] Vinnie Scarlata, Vinnie Johnson, Vinnie Beaney, and Piotr Zmijewski. *Supporting Third Party Attestation for Intel SGX with Intel Data Center Attestation Primitives*. Intel. https://www.intel.com/content/dam/develop/external/us/en/documents/intel-sgx-support-for-third-party-attestation-801017.pdf (Accessed 11 October 2022).

[40] Michael Schwarz, Moritz Lipp, Daniel Moghimi, Jo Van Bulck, Julian Stecklina, Thomas Prescher, and Daniel Gruss. ZombieLoad: Cross-Privilege-Boundary Data Sampling. In *CCS*, 2019.

[41] Alon Shakevsky, Eyal Ronen, and Avishai Wool. Trust Dies in Darkness: Shedding Light on Samsung's TrustZone Keymaster Design. In *31st USENIX Security Symposium (USENIX Security 22)*, pages 251–268, Boston, MA, August 2022. USENIX Association.

[42] Jo Van Bulck, Marina Minkin, Ofir Weisse, Daniel Genkin, Baris Kasikci, Frank Piessens, Mark Silberstein, Thomas F. Wenisch, Yuval Yarom, and Raoul Strackx. Foreshadow: Extracting the Keys to the Intel SGX Kingdom with Transient Out-of-Order Execution. In *USENIX Security Symposium*, 2018.

[43] Jo Van Bulck, Daniel Moghimi, Michael Schwarz, Moritz Lipp, Marina Minkin, Daniel Genkin, Yarom Yuval, Berk Sunar, Daniel Gruss, and Frank Piessens. LVI: Hijacking Transient Execution through Microarchitectural Load Value Injection. In *IEEE S&P'20*, 2020.

[44] Stephan van Schaik, Alyssa Milburn, Sebastian Österlund, Pietro Frigo, Giorgi Maisuradze, Kaveh Razavi, Herbert Bos, and Cristiano Giuffrida. RIDL: Rogue in-flight data load. In *IEEE S&P*, 2019.

[45] Stephan van Schaik, Alex Seto, Thomas Yurek, Adam Batori, Bader AlBassam, Christina Garman, Daniel Genkin, Andrew Miller, Eyal Ronen, and Yuval Yarom. SGX.Fail: How secrets get eXtracted. https://sgx.fail, 2022.

[46] Jan Werner, Joshua Mason, Manos Antonakakis, Michalis Polychronakis, and Fabian Monrose. The severest of them all: Inference attacks against secure virtual enclaves. In *CCS*, pages 73–85, 2019.

[47] Luca Wilke, Jan Wichelmann, Mathias Morbitzer, and Thomas Eisenbarth. SEVurity: No security without integrity: Breaking integrity-free memory encryption with minimal assumptions. In *IEEE SP*, pages 1483–1496, 2020.

[48] Ning Zhang, Kun Sun, Deborah Shands, Wenjing Lou, and Y Thomas Hou. TruSpy: Cache side-channel information leakage from the secure world on ARM devices. IACR Cryptology ePrint Archive 2016/980, 2016.

A Full Description

We provide in this section the full description in pseudo code of our proposal. Table 1 provides a summary of the cryptographic material used in our proposal. For each agent, we provide the multiple operations that can be performed. Local variables are written as x, while long term storage is denoted with x. Comments are written in gray. The API provided by the cryptographic library for the signature is shown in Fig. 5, the code of a TEE is in Fig. 6, the one of the provider is in Fig. 7, and the (very small) code of a third party checking an attestation is in Fig. 8.

```
Signature library S:
   Blind part
   (sk,pk) ←$ S.gen()
   blinded, skB ←$ S.blind(pk,m)
   blinded_sig ← S.bsign(sk,blinded)
   sig ← S.unblind(skB,pk,blinded_sig,m)
     return Null if invalid blinded
   Classical part
   sig ←$ S.sig(sk,m)
   S.vrfy(pk,sig) return bool

```

Figure 5: Signature Interface

B Communication Channel models

In this appendix, we provide more details on how a secure channel suitable for our protocols can be established as well as how we model it in Tamarin. We assume here basic knowledge about KEM, encryption, TLS, and Tamarin models.

```
Long term storage:
pkP: provisioning public key
    pkA: attestation public key
    SN: TEE serial number
    lt: linkable token
    ult: unlinkable token
    skT,pkT: Anonymous Certificate
    signed_pkT: pkT signed with pkA
    skNAC,pkNAC: Non Anonymous Cert
    signed_pkNAC: pkNAC signed with pkA

====================================
TEE Initialize(pkP,pkA,SN,lt)
------------------------------------
  Store all values in memory:
    (pkP,pkA,SN,lt) ← (pkP,pkA,SN,lt)

====================================
Linkable Chain
------------------------------------
 new unlinkable token
 t ←$ Token Space
 blinded, skB ←$ S.blind(pkP,t)
 new non anonymous cert
 skNAC,pkNAC ←$ S.gen()
 send authenticated with linkable token
 send Provider (SN, blinded, lt, pkNAC)
 receive (new_lt,bsig,sig_pkNAC)
 token_sig ← S.unblind(skB,pkP,bsig,t)
 abort if  token_sig is Null
 abort if not S.vrfy(pkA,sig_pkNAC)
 if success, store vars
 ut ← (t,token_sig)
 lt ← new_lt
 signed_pkNAC ← sig_pkNAC

====================================
Unlinkable Chain
------------------------------------
 new unlinkable token
 t ←$ Token Space
 bt, skB ←$ S.blind(pkP,t)
 new anonymous cert
 nskT,npkT ←$ S.gen()
 bT, skBT ←$ S.blind(pkA,pkT)
 send all authenticated with previous
 blind token
 send Provider (bt, bT, ut)
 receive (bisgt,bsigT)
 token_sig ← S.unblind(skB,pkP,bsigt,t)
 abort if  token_sig is Null
 npkT_sig ← S.unblind(skBT,pkA,bsigT,npkT)
 abort if  npkT_sig is Null
 if success of unblind, store vars
 ut ← (nt,ntoken_sig)
 skT,pkT ← nskT, npkT
 signed_pkT ← npkT_sig

====================================
Anonymous Attest(m)
 sig ← S.sign(skT,m)
 sent to TTP (m,sig,pkT, signed_pkT)

====================================
Non Anonymous Attest(m)
 sig ← S.sign(skNAC,m)
 sent to TTP (m,sig,pkNAC, signed_pkNAC)

====================================
Refresh keys
 Upon expiry, fetch new pkP,pkA, e.g.,
 relying on provider's TLS cert.
 Drop all expired signatures and run
 linkable chain.
```

Figure 6: TEE specification

Formal Model

Our protocol and our proofs rely on a channel that is:

- unilaterally authenticated and confidentiality protected: any message sent over it will be delivered as is to the Provider;
- unlinkable: two distinct sessions of the same clients are not related at all.

We formally model this in Tamarin using classical channel modelings, similar e.g. to the one of [4]. Our confidential channels are however simplified, as there is a single receiver, the provider.

Without going into the details of the Tamarin notation, we can describe how our formal models capture the following possible actions for the communication channel between clients and a single authenticated server:

- A client can sample a fresh identifier id, and secretly transmit once to the Provider a pair (id, m). Such transmission can only be delayed by the attacker.
- The server, if it knows a particular id, can send a single reply to the client.
- The attacker can chose its own identifier id and also send a message to the server.
- The server answers to the attacker when an attacker identifier was received.

```
Long term storage:
    skP,pkP: provisioning key pair
    skA,pkA: attestation key pair
    dlts: deprecated unlinkable tokens
    lts: valid linkable tokens

====================================
ProviderInitialize()
------------------------------------
 skP,pkP <-$- S.gen()
 skA,pkA <-$- S.gen()

====================================
Create TEE(SN)
------------------------------------
 lt <-$- Token Space
 Make TEE execute:
  TEE Initialize(pkP,pkA,SN,lt)
 lts <- lts + (SN,lt)

====================================
Linkable Chain
------------------------------------
 receive from non authenticated client
 receive  (SN, blinded, lt, pkNAC)
 abort if (SN,lt) is not in lts
 new_lt <-$- Token Space
 lts <- lts - (SN,lt) + (SN,new_lt)
 bsig <- S.bsign(skP,blinded)
 sig_pkNAC <- S.sign(skA,pkNAC)
 send (new_lt,bsig,sig_pkNAC)


====================================
Unlinkable Chain
------------------------------------
 receive from non authenticated client
 receive (bt, bT, (t,sigt))
 Check validity of blind token
 abort if not Sig.vrfy(pkP,sigt,t)
 Check t not in dlts
 dlts <- dlts + t
 bsigt <-$- S.bsign(skP,bt)
 bsigT <-$- S.bsign(skA,bT)
 send (bsigt,bsigT)

====================================
Key Refresh()
------------------------------------
 Upon expiry, run ProviderInitialize().
 Publish new public keys.
```

Figure 7: Provider specification

```
====================================
Check attest()
------------------------------------
 receive (m,sig,pkNAC, signed_pkNAC)
 Fetch current attestation
 key pkA from provider.
 abort if not
     S.vrfy(pkA,  signed_pkNAC, pkNAC)
 abort if not S.vrfy(pkNAC, sig,m)
 Accept
```

Figure 8: Third Party

Realization

Such a channel can be for instance established by using the TLS protocol, to avoid managing an additional certificate on the provider side. Then, for each loop of Section 5.2, the TEE starts a fresh TLS handshake with the provider and use the TLS session as a channel. And for each loop of Section 5.3, another fresh TLS handshake is also used. Implementers must take care not to use any session resumption mechanism, which would otherwise compromise trivially unlinkability.

If TLS is too heavyweight for the use-case constraints, a simple communication channel can be established as follows by relying on a KEM and a symmetric encryption :

- the provider has a long term KEM key pair $(\mathsf{pk}, \mathsf{sk})$;
- any client that wants to send a message m to the provider first executes $\mathsf{sk}_t, ec_t \leftarrow \mathtt{Encap}(\mathsf{pk})$, and then sends on the network the pair $(ec_t, \mathtt{Enc}((1, m), \mathsf{sk}_t)$.
- the provider given (ec_t, em) obtains the key $\mathsf{sk}_t \leftarrow \mathtt{Decap}(ec_t, \mathsf{sk})$, and decrypts the message with $\mathtt{Dec}(em, \mathsf{sk}_t)$. It can then process it, and finally answer to the client with message m_2 by sending back $\mathtt{Enc}((2, m_2), \mathsf{sk}_t)$.

Name	Description
Serial Number (SN)	The serial number of a TEE
Non Anonymous Certificate (NAC)	An attestation certificate e.g. tied to the SN, used by the TEE to attest itself to third party servers
Anonymous Certificate (AC)	An attestation certificate but fully anonymous
Authorization token	A one-time authorization token, where upon each authorization a new token is delivered
Linkable Token	An authorization token owned by the TEE, linked to its SN and valid for the provider
Unlinkable Token	An authorization token owned by the TEE and blindly signed by the provider
Attestation key pair $(\mathsf{sk}_A, \mathsf{pk}_A)$	Key trusted by third parties to sign ACs and NACs
Provisioning key pair $(\mathsf{sk}_P, \mathsf{pk}_P)$	Key used by the provider to sign Unlinkable Token

Table 1: Cryptographic Material Summary

Parameters:	n TEEs	m_l linkable updates	m_u unlinkable updates	Result
	2	8	8	ok in 54s, 68MB
	2	12	24	OOM>500GB in 10m
	2	12	12	ok in 19h29m, 23GB

Figure 9: DeepSec analysis results

Secure Handling of Communication issues and TEE reset

In our formal models and descriptions, we implicitly assume that the connection between the provider and a TEE cannot be lost but only delayed. In practice, we need to support scenarios where the connection with the TEE is lost after the provider sends the new blinded signature but *before* it was received by and stored by the client. If the provider doesn't accept the old token anymore, an honest TEE who didn't get the new blinded signature will be locked out. If it accepts the old token, a malicious client may get two or more valid tokens in exchange for one.

Suppose we use the previously proposed KEM based approach for the secure channel implementation. In that case, the solution is trivial as the clients and server just need to replay the message previously sent using the same encryption keys to avoid any message loss.

Another solution if TLS is used is simply to rely on the session resumption mechanism of TLS (but only within the same linkable or the same unlinkable update). As soon as the server gets a valid token, it marks the corresponding TLS session as valid and sends and stores its reply. If this TLS session is resumed from a client, it accepts to resend the stored reply.

C Formal details on the privacy proof

In this appendix, while we cannot re-introduce formally all the notions needed to fully explain to a new reader the formal details of our proofs, we present all the required notions and give precise references for them.

Unlinkability properties

In the formal methods community, a common privacy goal is the so-called unlinkability property, informally defined in [24] as: "Unlinkability aims at ensuring that a user may make multiple uses of a service or resource without others being able to link these uses together." It is a stronger goal than anonymity but difficult to prove and multiple works have tried to define it formally and enable proving it [1, 3, 23]. An important notion in the field is the *trace equivalence* [3, Def. 2] property, which allows to specify that two protocols have exactly the same set of possible executions, and that those executions are indistinguishable by any attacker. We denote $P \approx Q$ the fact that a protocol P is trace-equivalent to a protocol Q. Given a protocol $P(id)$ where id corresponds to the identifier of an agent involved in the protocol, if we denote $\|$

the parallel composition of session, the unlinkability of the agents in the protocol P is expressed as:

$$P(id)\| \dots \|P(id) \approx P(id_1)\| \dots \|P(id_n)$$

That is, an attacker cannot distinguish whether it was n times the same agent that was involved in the n sessions of the protocol or n distinct agents. This implies that the attacker cannot link together two sessions of the same user.

Unlinkability definition of TokenWeaver

Our goal is to verify the privacy of our solution, even for a malicious server trying to track the TEEs. As such, we will consider here that the server is fully attacker controlled, and the unlinkability property will only talk about the parts of the protocol executed by the TEEs.

A difficulty of specifying the unlinkability property for our protocol is that it has both unlinkable and linkable components. Let us introduce some notations to clarify this. We split our protocol for the TEE side into three component:

- $\mathsf{Init}(SN)$ - A TEE with serial number SN is given a linkable token;
- $\mathsf{UUpdate}(SN)$ - The TEE with id SN tries to perform an unlinkable update, sending out its unlinkable token (if it has one) and a request for a new AC.
- $\mathsf{LUpdate}(SN)$ - The TEE SN sends out its linkable token, and should obtain a new one along with a blinded token.

Those three protocol parts all share the common state of the TEE SN, and cannot be interwoven together. A first attempt at defining the unlinkability of our protocol could be, when only considering two TEEs:

$$\begin{gathered}\mathsf{Init}(SN_1)\|\mathsf{UUpdate}(SN_1)\|\mathsf{LUpdate}(SN_1)\\ \|\mathsf{Init}(SN_1)\|\mathsf{UUpdate}(SN_1)\|\mathsf{LUpdate}(SN_1)\\ \approx\\ \mathsf{Init}(SN_1)\|\mathsf{UUpdate}(SN_1)\|\mathsf{LUpdate}(SN_1)\|\\ \mathsf{Init}(SN_2)\|\mathsf{UUpdate}(SN_2)\|\mathsf{LUpdate}(SN_2)\end{gathered}$$

This property is however trivially false, as for instance the sequence of actions $\mathsf{LUpdate}(SN_1).\mathsf{LUpdate}(SN_2)$ is of course distinguishable from the sequence of actions $\mathsf{LUpdate}(SN_1).\mathsf{LUpdate}(SN_1)$. This property does not correspond to a satisfying definition of unlinkability for our setting.

The natural next option is to only consider the unlinkability for the parts of the protocol that are indeed unlinkable, as follows:

$$\begin{gathered}\mathsf{Init}(SN_1)\|\mathsf{UUpdate}(SN_1)\|\mathsf{LUpdate}(SN_1)\\ \|\mathsf{Init}(SN_2)\|\mathsf{UUpdate}(SN_1)\|\mathsf{LUpdate}(SN_2)\\ \approx\\ \mathsf{Init}(SN_1)\|\mathsf{UUpdate}(SN_1)\|\mathsf{LUpdate}(SN_1)\|\\ \mathsf{Init}(SN_2)\|\mathsf{UUpdate}(SN_2)\|\mathsf{LUpdate}(SN_2)\end{gathered}$$

While this would work for a stateless protocol, this is still not a valid definition of unlinkability in our setting as it is also trivially false. Indeed, the sequence $\mathsf{LUpdate}(SN_1).\mathsf{UUpdate}(SN_1).\mathsf{UUpdate}(SN_1)$ is possible on the left hand side, but the correspond one on the right hand side, which would be $\mathsf{LUpdate}(SN_1).\mathsf{UUpdate}(SN_1).\mathsf{UUpdate}(SN_2)$, is an impossible execution, as $\mathsf{UUpdate}(SN_2)$ cannot be triggered without a corresponding $\mathsf{LUpdate}(SN_2)$. This in fact matches the intuition that in the real world, only devices that did perform the latest linkable update are unlinkable. Unfortunately, the existing state of the art tools do not allow us to accurately express such a property.

We however go around the issue by restricting the scope of our analysis: we only express unlinkability over a system where we forces all TEEs to perform at the same time the linkable update.

We now denote $\mathsf{LUpdate}(SN_1, \dots, SN_n)$ the protocol where all the TEEs perform one after another the linkable update, and none of those TEEs launch any other action during this global update. We can then express our unlinkability target, in the specific case of only two TEEs performing a single linkable and unlinkable update, as:

$$\begin{gathered}\mathsf{Init}(SN_1)\|\mathsf{Init}(SN_2)\|\mathsf{LUpdate}(SN_1, SN_2)\\ \|\mathsf{UUpdate}(SN_1)\|\mathsf{UUpdate}(SN_2)\\ \approx\\ \mathsf{Init}(SN_1)\|\mathsf{Init}(SN_2)\|\mathsf{LUpdate}(SN_1, SN_2)\\ \|\mathsf{UUpdate}(SN_1)\|\mathsf{UUpdate}(SN_1)\end{gathered}$$

We then generalize this property to a number of TEEs n, a number of possible linkable updates m_l, and a number of possible unlinkable updates m_u by using the notation $\|_{1\leq i\leq m} P_i$ to denote $P_1\| \ldots \|P_m$ and writing it as:

$$\|_{1\leq i\leq n}\mathsf{Init}(SN_i)\|_{1\leq j\leq m_l}\mathsf{LUpdate}(SN_1,\ldots,SN_n)$$
$$\|_{1\leq k\leq m_i}\mathsf{UUpdate}(SN_k) \approx$$
$$\|_{1\leq i\leq n}\mathsf{Init}(SN_i)\|_{1\leq j\leq m_l}\mathsf{LUpdate}(SN_1,\ldots,SN_n)$$
$$\|_{1\leq k\leq m_i}\mathsf{UUpdate}(SN_1)$$

Our unlinkability property then captures the fact that for n TEEs that all performed the same number of linkable updates, an attacker cannot distinguish whether it is always the same TEE or always a distinct one which is doing an unlinkable update.

Actual Verification

Because our unlinkability property is not as simple as the classical one and involves non unlinkable components, we cannot reuse solutions dedicated to a particular specification of unlinkability such as [3].

We thus have to resort to general tools that support the verification of trace equivalence. In this work, we rely on one of the latest development in this field, the DeepSec prover [11, 12], which allows verifying trace equivalence between two given protocols. While DeepSec is a state-of-the-art tool, it puts two restrictions on our analysis:

- it does not have built-in support for states, and we must use private communication channels to emulate them. However, while the content of messages sent over private channels is unknown to the attacker, the attacker can observe that a communication occurred over a channel. Thus, if we were to encode each TEE state as one private channel, the attacker would instantly distinguish $\mathsf{UUpdate}(SN_1)\|\mathsf{UUpdate}(SN_2)$ and $\mathsf{UUpdate}(SN_1)\|\mathsf{UUpdate}(SN_1)$, as in the first case a single private channel is used, and in the second two are used. We solve this by using a single private channel to encode the joint states of all TEEs as a tuple, and a given protocol will only touch the part of the tuple corresponding to the given TEE. This however makes it so that our protocol model is not at all modular in the number of different TEEs n in the proof, and we thus only restrict it to 2 instances.
- DeepSec only enables verification for a bounded number of sessions, and the complexity of the verification grows exponentially with the number of sessions.

We provide in Fig. 9 the summary of our results, with some timeouts and out of memory occurrences to give an idea of the limits.