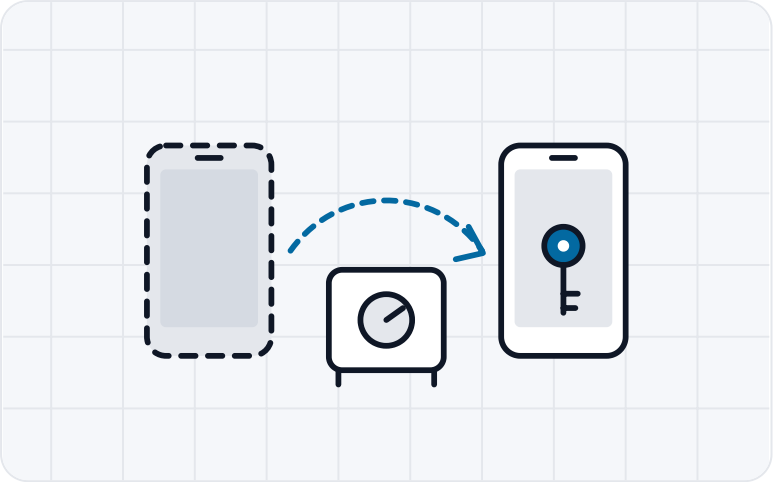
A-SIT Technology

E-Government Innovationszentrum

21. Dezember 2023 Konzept · Digitale Identität · Privatsphäre & Krypto · 18 Min. Lesezeit

Wiederherstellung von Identitäten bei Geräteverlust

Stefan More



Autorinnen und Autoren	Stefan More
Quelle	https://technology2.a-sit.at/veroeffentlichungen/wiederherstellung-von-identitaeten-bei-geraeteverlust/
Hinweis	Maschinell übersetzt.

Kernaussagen

- Eine physische Identität ist gerätegebunden und nie übertragbar; ein Backup mit Wiederherstellung ist nur für logische Identitäten möglich.
- Bei Identity Re-Issuing verlässt kein Schlüsselmaterial das Gerät: Die logische Identität wird wiederhergestellt, die physische Identität des Geräts ist neu.
- Hybrid Recovery kombiniert beide Arten, etwa mit Device-Binding-Credentials, die Gerätschlüssel und Credentials verbinden.
- Daten werden nie im Klartext exportiert; Proxy Re-Encryption gibt Zielgeräten Zugriff, ohne dass die Storage-Komponente Daten sieht.
- Ein Prototypdesign mit TEE und zwei IOT-Geräten zeigt die Umsetzbarkeit des Backup-und-Recovery-Systems.

Die zunehmende Verbreitung digitaler Identitäten und kryptografischer Schlüsselmaterialien auf unterschiedlichen Geräten birgt ein hohes Sicherheitsrisiko. Wenn ein Gerät verloren geht oder gestohlen wird, können die darauf gespeicherten Identitäten und Schlüsselmaterialien in die Hände Unbefugter gelangen. Um dieses Risiko zu minimieren, kommen Hardware-unterstützte Techniken zum Einsatz, um das Schlüsselmaterial zu schützen. Diese Techniken verhindern beispielsweise, dass eine Malwareauf das sensitive Material zugreifen kann.

Ein Problem ist, wenn diese Geräte verloren gehen oder gestohlen werden, und ein/e Benutzer:in dadurch den Zugriff auf seine digitale Identität verliert. Ziel dieses Projekts ist die weitere Erforschung von Systemen und Mechanismen für das Backup und Recovery von kryptografischem Schlüsselmaterial sowie weitere Verfahren zum Wiederherstellen von Identitäten. Das Ziel dieses Forschungsprojekts ist es, einen Weg zu finden, um in einem TEE gespeicherte Identitäten und Schlüssel sicher zu sichern und wiederherzustellen, so dass die Identitäten nicht verloren gehen, wenn das Gerät verloren geht.

1. Einleitung

Digitale Identitäts-Wallets sind eine aufkommende Technologie, mit der Benutzer:innen ihre Identitätsdaten souverän speichern und verwenden können. Typische Beispiele sind Anwendungsfälle wie elektronische Identitäten (eID), akademische Abschlüsse, Fahrausweise im öffentlichen Verkehr und andere Formen von Zertifizierungen und Zugangsberechtigungen. Mit der Metapher einer physischen „Brieftasche“, die Ausweise und Nachweise verschiedener Art enthält, wollen Identitäts-Wallets zu einem zentralen Ort im (digitalen) Leben aller werden. Anders als physische Brieftaschen können „digitale Identitäts-Wallets“ digitale Funktionen nutzen, etwa das Vorzeigen von Nachweisen aus der Ferne, sowie moderne kryptografische Konzepte, etwa datenschutzfördernde Technologien. Ebenso müssen digitale Wallets die Besonderheiten digitaler Systeme berücksichtigen. Vor allem kann ein digitaler Nachweis (Credential), da er nur aus Daten besteht, (absichtlich oder böswillig) unbegrenzt kopiert werden.

Dies verletzt die Annahme bei den physischen Gegenstücken, bei denen das Kopieren (oder Fälschen) eines Nachweises entweder unmöglich oder zumindest schwierig ist. Viele Anwendungsfälle beruhen darauf, dass ein Nachweis nur ein einziges Mal existieren kann, und manche gehen auch davon aus, dass es nicht einfach ist, einen Nachweis an eine andere Person zu übertragen. Das muss beim Entwurf eines Systems auf Basis digitaler Identitäts-Wallets berücksichtigt werden. Um diese Anforderung zu erfüllen, gibt es Technologien, die den Export kryptografischer Daten aus einem Gerät verhindern und es Benutzer:innen dennoch erlauben, sie für digitale Austauschvorgänge zu verwenden. Beispiele sind Trusted Execution Environments (TEE), Hardware Security Modules (HSM) und Secure Elements (SE). Einige Betriebssysteme bieten auch Systeme zur Verwaltung und Nutzung kryptografischer Schlüssel mit solchen Hardware-Technologien, zum Beispiel das Keystore-System von Android. [1] Ebenso verwenden Geräte des Internets der Dinge (IOT) ihre Geräteidentitäten, um sich bei Update-Servern, in ihrer Verwaltungsdomäne oder gegenüber anderen Geräten zu authentifizieren. Dazu nutzen sie kryptografische Schlüssel und Nachweise, die oft mit den oben genannten sicheren Hardware-Technologien verwaltet werden. Das Ergebnis ist eine Identität, die an das jeweilige Gerät gebunden ist und nicht übertragen werden kann.

Geräte werden jedoch ersetzt und Telefone gehen kaputt, was möglicherweise zum Verlust des Zugriffs auf die auf dem Gerät gespeicherten Identitätsdaten führt. Außerdem können Telefone gestohlen oder gehackt werden und Geräte verloren gehen, was eine weitere Bedrohung für die Verfügbarkeit und Vertraulichkeit der Identitätsdaten darstellt.

2. Arten von Identitäten

Im Kontext von Identitätsdaten, die auf mobilen und IOT-Geräten gespeichert sind, werden die folgenden Arten von Identitätsdaten unterschieden:

2.1. Physische und logische Identitäten

Eine physische Identität ist eine Identität, die an ein bestimmtes physisches Gerät gebunden ist. Da Identitäten üblicherweise durch kryptografische Schlüssel und Nachweise dargestellt werden, bedeutet das, dass der (private) Schlüssel dazu dient, den Besitz bzw. die Inhaberschaft der Identität nachzuweisen. Um den privaten Schlüssel an das Gerät zu binden, wird der Schlüssel auf dem Gerät gespeichert[1] und zwar so, dass er das Gerät nicht verlassen kann.[2] Dies geschieht üblicherweise mithilfe sicherer Hardware-Funktionen, z. B. eines TEE.









Eine logische Identität ist dagegen nicht an ein bestimmtes physisches Gerät gebunden. Stattdessen stellt sie in manchen Anwendungsfällen eine höhere Abstraktion der Identität des Geräts dar. Beispiele sind die Rolle des Geräts in einem Anwendungsfall oder die Identitätsdaten eines dritten Geräts, das von diesem Gerät verwaltet wird (selbst aber keine Möglichkeit hat, die Identitätsdaten zu speichern). Außerdem werden im Kontext digitaler Identitäten auf mobilen Geräten logische Identitäten verwendet, um die Identität einer (natürlichen oder juristischen) Person darzustellen. Im letzteren Fall repräsentieren die Identitätsdaten nicht das physische Gerät, können aber dennoch gerätegebunden sein, wenn Vorschriften dies verlangen. Im Kontext dieses Berichts wird zwischen gerätegebundenen (physischen) und übertragbaren (logischen) Identitäten unterschieden.

Im Kontext von Backup und Recovery besteht der Unterschied zwischen den beiden Arten von Identitäten darin, dass die physische Identität eines Geräts nie auf ein zweites Gerät übertragen werden kann, selbst wenn dieses zweite Gerät die Funktionalität und Rolle des ersten vollständig ersetzt. Verlangt ein Anwendungsfall dies, müssen logische Identitäten verwendet werden. Physische Identitäten können in diesen Anwendungsfällen dennoch eine Rolle spielen, da sie die sichere Wiederherstellung logischer Identitäten unterstützen können.

2.2. Credentials und Schlüssel

Credentials sind Datenstrukturen, die eine Menge von Attributen über ein Datensubjekt (z. B. eine Person oder ein Gerät) enthalten. Sie dienen dazu, Identitätsdaten zu kodieren, und werden auf einem Mobiltelefon oder IOT-Gerät (dem Holder) gespeichert. Um Authentizität und Integrität zu gewährleisten, werden Credentials von einem Aussteller (Issuer) kryptografisch signiert.

Kryptografische Schlüssel dienen dazu, den Besitz eines Credentials nachzuweisen. Dies geschieht üblicherweise, indem der öffentliche Schlüssel in das Credential eingebettet wird. Beim Vorzeigen eines Credentials signiert der Holder dann mit seinem privaten Schlüssel eine Challenge, die der Dienst, der das Credential angefordert hat, vorgibt.

2.3. Weitere Daten

Weitere Arten von Identitäten und Identitätsdaten, die den Backup- und Recovery-Mechanismen unterliegen, sind:

- Dezentrale Identifikatoren (Decentralized Identifiers, DIDs) sind Identifikatoren, die im Modell der (selbst-)souveränen Identität üblich sind. Sie werden durch einen Identifikator dargestellt, der auf unterschiedlichen Wegen in das zugehörige Schlüsselmaterial aufgelöst werden kann. Mit ihnen lassen sich entweder logische oder physische Identitäten kodieren. Anders als Credential-basierte Identitäten enthalten DIDs außer kryptografischen Schlüsseln und anderen technischen Informationen, die zur Authentifizierung des Identitätssubjekts nötig sind, keine Informationen (d. h. Attribute) über das Subjekt. Im Kontext von Backup und Recovery unterliegen die zur DID gehörenden (privaten) Schlüssel jedoch denselben Wiederherstellungsanforderungen wie das Schlüsselmaterial von Credentials.
- Andere Daten, die zum Betrieb des Geräts oder der Wallet nötig sind, etwa Enrollment-Informationen oder Konfigurationsdaten. Je nach Anwendungsfall sind diese Daten gerätespezifisch (dann ist kein Backup erforderlich) oder allgemeiner und an die logische Identität gebunden (dann ist ein Backup wichtig).

3. Identitätswiederherstellung

In diesem Bericht werden die folgenden Definitionen für die beteiligten Komponenten verwendet. Diese Komponenten und ihr Zusammenhang sind auch in Abbildung 1 unten dargestellt.

- Gerät: Ein IOT-Gerät oder Smartphone, das zum Speichern, Verwalten und Vorzeigen digitaler Identitäten dient. Im Kontext dieses Berichts werden die sensiblen Informationen (d. h. kryptografisches Material) geschützt auf dem Gerät gespeichert (z. B. mithilfe eines TEE). Das Gerät kann auch andere Funktionen erfüllen, für die es Identitätsinformationen benötigt.

    - Quellgerät (Source Device): Ein Gerät, das durch ein anderes Gerät (das entsprechende Zielgerät) ersetzt werden soll, falls es nicht mehr verfügbar ist (z. B. defekt, fehlerhaft, verloren, gestohlen, ...).
    - Zielgerät (Target Device): Das Gerät, das das Quellgerät ersetzt. Im Allgemeinen hat das Zielgerät dieselben Hardware- und Softwarefähigkeiten wie das Quellgerät, das es ersetzt. Kleine Abweichungen sind jedoch möglich, solange die Kernfunktionalität vorhanden ist, die das wiederhergestellte System und das Recovery-System benötigen.
- Identity Backup and Recovery System (B&R): Alle Systeme, die für einen Identitätswiederherstellungsprozess nötig sind. Dazu gehören Softwarekomponenten sowohl auf dem Quellgerät als auch auf dem Zielgerät (B&R-Client). Außerdem gibt es weitere Komponenten in der Gesamtarchitektur des Systems, z. B. einen Dateiserver zum Speichern der Backups, ein Gerät (und Software) zur Steuerung des Wiederherstellungsprozesses und das Netzwerk, das alle Komponenten verbindet.
    - Management-Komponente: Die Komponente zur Steuerung des Backup- und Recovery-Prozesses. Die Administrator:innen des Systems verwenden sie, um neue Geräte zu registrieren (Enrollment), kryptografische Schlüssel einzurichten, den Backup-Speicherort (d. h. die Storage-Komponente) zu konfigurieren und einen Wiederherstellungsprozess zu starten. Je nach konkretem Anwendungsfall kann die Management-Komponente beispielsweise ein Server mit Weboberfläche oder eine App auf dem Telefon der Administrator:innen sein. Diese Komponente verwaltet die kryptografischen Schlüssel für das Backup- und Recovery-System, speichert aber nicht zwingend die eigentlichen Daten. Sie ist daher eine leichtgewichtige Komponente, die nicht ständig online sein muss, aber höhere Anforderungen an Vertrauen und Sicherheit stellt, da sie den Zugriff auf sensible Daten steuert.
    - Storage-Komponente: Die Komponente, die die gesicherten Identitätsinformationen speichert, vom Quellgerät empfängt und an das Zielgerät sendet. Zusätzlich führt sie die Zugriffskontrolloperationen durch, die nötig sind, um die (geschützten) gesicherten Daten für das Zielgerät verfügbar zu machen. Je nach Gesamtarchitektur können die Management-Komponente und die Storage-Komponente zu einer einzigen Komponente zusammengefasst werden. Anders als die Management-Komponente muss die Storage-Komponente ständig verfügbar und online sein, damit Geräte neue Backup-Snapshots übermitteln können. Da sie Identitätsdaten nie im Klartext empfängt oder verarbeitet, stellt sie geringere Anforderungen an Vertrauen und Sicherheit als das Management-Gerät.

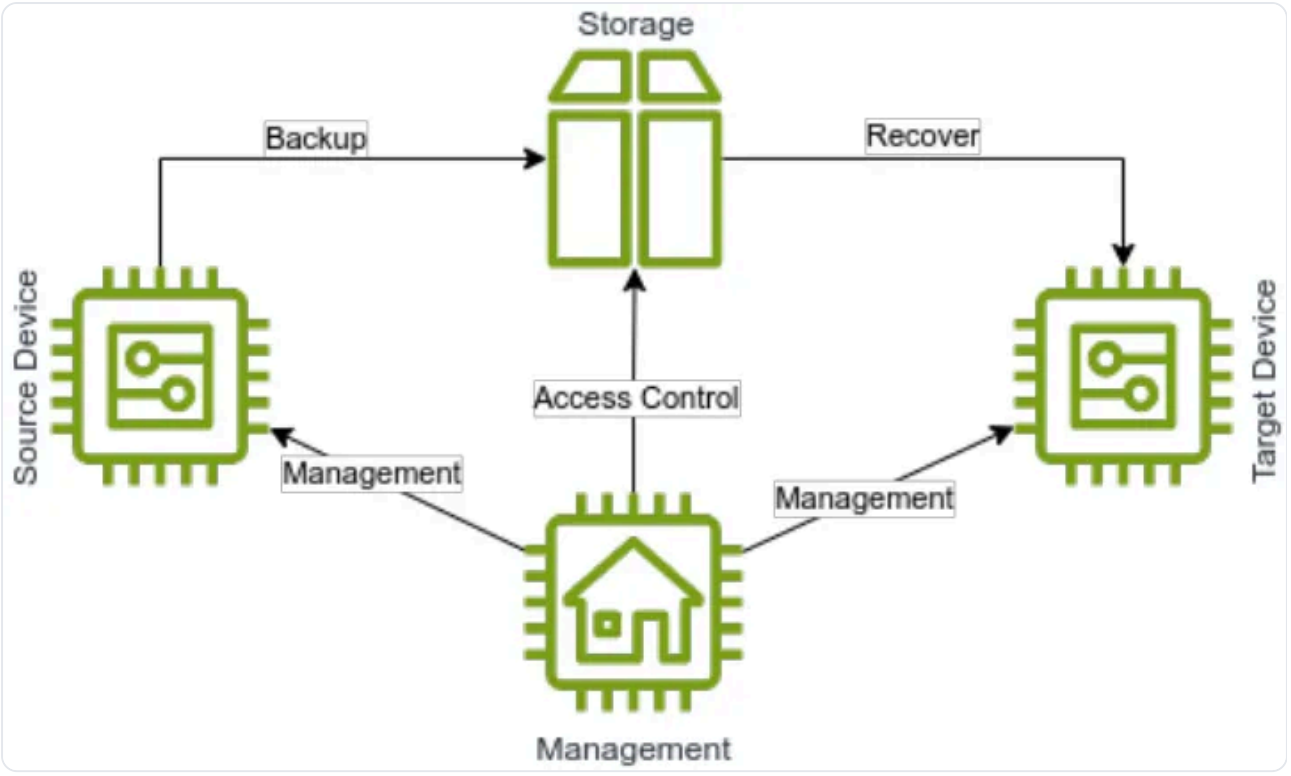


Abbildung 1: Überblick über die B&R-Komponenten und ihren Zusammenhang

Es werden zwei Fälle unterschieden, in denen eine Identitätswiederherstellung nötig ist:

- Fall 1 ermöglicht die Wiederverwendung der Identität des Quellgeräts, während das Gerät regulär ersetzt wird, z. B. bei einer planmäßigen Wartung. In diesem Fall existieren Quell- und Zielgerät gleichzeitig.
- Fall 2 ermöglicht die Wiederherstellung der geschützten Identitätsdaten, auch wenn das Quellgerät nicht mehr verfügbar ist. In diesem Fall existiert das Zielgerät erst, nachdem das alte Gerät nicht mehr verfügbar ist, sodass kein direkter Übertragungsprozess möglich ist. Da dies der allgemeinere Fall ist, lösen Lösungen für Fall 2 auch Szenarien von Fall 1.

3.1. Arten der Identitätswiederherstellung

Im Folgenden werden verschiedene Arten der Identitätswiederherstellung beschrieben. Alle hier behandelten Arten der Identitätswiederherstellung decken beide oben beschriebenen Wiederherstellungsfälle ab.

3.1.1. Identity Backup and Restore

Bei dieser Art exportiert das Quellgerät die Identitätsdaten fortlaufend in den B&R-Speicher. Fällt das Gerät aus, wählen die Administrator:innen des Systems mit der Management-Komponente einen geeigneten Backup-Snapshot aus und importieren ihn auf das Zielgerät. Der B&D-Client auf dem Zielgerät importiert dann die Identitätsdaten in den sicheren Speicher des Geräts. Dadurch verwendet das Zielgerät das kryptografische Material und die Credentials des Quellgeräts wieder und übernimmt so die logische Identität des Quellgeräts.

Für einen sicheren Backup- und Recovery-Ablauf ist es erforderlich, dass keine unbefugte Partei Zugriff auf die gesicherten Daten hat. Das ist besonders wichtig, da die aus den Geräten exportierten Daten aus der sicheren Speicherkomponente des Geräts stammen und ein ungeschützter Export diese Datenschutzschicht durchbrechen würde. Um diese Anforderung zu erfüllen, werden die Daten nie im Klartext aus dem sicheren Speicher exportiert und nur verschlüsselt übertragen und gespeichert. Außerdem wird großer Wert darauf gelegt, dass auch die zur Verschlüsselung der Daten verwendeten Schlüssel geschützt und sicher verwaltet werden, damit nur berechtigte Stellen (d. h. das autorisierte Zielgerät) die Daten entschlüsseln können. Die kryptografischen Mechanismen, die dieses sichere Backup und Restore ermöglichen, werden in Abschnitt 4.3 unten behandelt.

Eine vollständige Identitätswiederherstellung mittels Identity Backup and Restore ist nur für logische Identitäten möglich, da physische Identitäten gerätegebunden sind und ihr zugehöriger (privater) Schlüssel daher nicht gesichert und aus dem Gerät exportiert werden kann.

3.1.2. Identity Re-Issuing

Die Alternative zu einem vollständigen Backup und Restore der Identitätsdaten ist ein eher logischer Wiederherstellungsprozess. Bei dieser Art der Identitätswiederherstellung verlassen die kryptografischen Daten, die zu den Identitätsinformationen gehören, das Gerät nie. Das kann der Fall sein, wenn die Identitätsdaten auf einer Form gerätegebundener Identität beruhen oder wenn das Gerät seine Identitätsdaten nicht exportieren kann. Bei dieser Art wird die Identität des Zielgeräts neu eingerichtet, z. B. durch Systemadministrator:innen.

Dazu wird zunächst das Zielgerät im System registriert (Enrollment). Anschließend konfiguriert das Management-Gerät neues kryptografisches Material auf dem Zielgerät und erzeugt es. Nach der Authentifizierung des Geräts oder seiner Inhaber:in wird dieses kryptografische Material verwendet, um neue Identitätsinformationen, d. h. Credentials, erneut auszustellen. Da die Management-Komponente Identitätsinformationen des Quellgeräts wiederverwenden bzw. ausstellen kann, stellt dies die alte Identität auf dem Zielgerät faktisch wieder her. Dadurch wird die logische Identität wiederhergestellt, die physische Identität des Geräts ist jedoch eine neue.

3.1.3. Hybrid Recovery

Eine dritte Art der Identität ist eine Kombination der beiden oben beschriebenen Arten.

Eine Form besteht darin, nur Teile der Identitätsinformationen auf das Zielgerät zu übertragen und mit diesen Informationen alle übrigen (gerätegebundenen) Identitätsinformationen neu auszustellen und an das neue Gerät zu binden.

Eine andere Form der Hybrid Recovery besteht darin, Identitätsinformationen nie an ein physisches Gerät zu binden, sondern stattdessen Device-Binding-Credentials einzuführen, die dies leisten. In diesem Szenario können Identitätsdaten einfach auf das neue Gerät übertragen werden (z. B. mit dem in Abschnitt 3.1.1 oben beschriebenen Mechanismus). Um die Verbindung zwischen Gerät und Identität herzustellen und damit den Besitznachweis (wieder) zu ermöglichen, registriert die Management-Komponente das Gerät manuell und stellt ihm ein Device-Binding-Credential aus, das den Schlüssel des Geräts mit den Credentials verbindet.

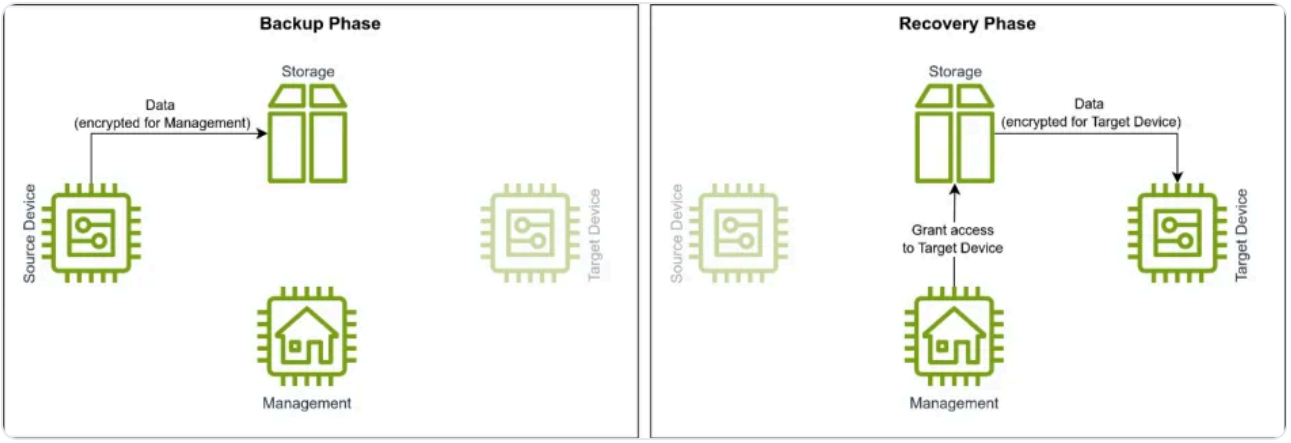


Abbildung 2: Konzeptioneller Überblick über die B&R-Phasen

4. Technische Aspekte

In diesem Abschnitt werden die technischen Aspekte der sicheren Identitätswiederherstellung behandelt. Im Einzelnen liegt der Fokus auf der Speicherung von Identitätsinformationen auf dem Gerät, auf der Bindung einer Identität an ein bestimmtes Gerät sowie auf kryptografischen Mechanismen, die die Identitätsinformationen im Backup- und Recovery-Prozess schützen.

4.1. Sichere Speicherung von Identitätsinformationen

Identitätsinformationen enthalten oft personenbezogene Daten und sind daher sensible Informationen, die geschützt werden müssen, um Datenschutzvorschriften einzuhalten und die Privatsphäre der betroffenen Personen zu sichern. Ebenso können Identitätsinformationen von Geräten als sensibel gelten, z. B. wenn sie genutzt werden können, um Zugang zu personenbezogenen Informationen oder Zugriff auf andere kritische Ressourcen und deren Kontrolle zu erlangen. Es ist daher wichtig, dass auf Geräten gespeicherte Identitätsinformationen im Betrieb geschützt sind. Das konkrete Bedrohungsmodell hängt vom Anwendungsfall und der Umgebung des Geräts ab.

Smartphones können beispielsweise verloren gehen oder gestohlen werden, und Angreifer:innen oder Dieb:innen sollen daran gehindert werden, auf die Identitäts-Wallet der Benutzer:in zuzugreifen. Das kann schwierig sein, da die böswillige Stelle physischen Zugriff auf das Gerät hat und dessen Speicher und manchmal sogar den Arbeitsspeicher lesen kann. Um diese Art unbefugten Zugriffs zu verhindern, sollten Wallet-Systeme als Mindestmaßnahme die Datei- und Festplattenverschlüsselung des Betriebssystems nutzen, um ruhende sensible Daten zu schützen und sie aus dem Arbeitsspeicher des Geräts zu entfernen, wenn das Gerät gesperrt ist. Außerdem sollten Benutzer:innen dieser Apps dazu angehalten werden, die Sicherheitsmaßnahmen des Geräts zu nutzen, z. B. eine Gerätesperre einzurichten und stets die neuesten Updates zu installieren.

Weitere häufige Bedrohungen für die Sicherheit von Identitätsdaten sind schädliche Apps oder Malware sowie Apps mit Softwareschwachstellen, die sensible Identitätsdaten verarbeiten. Ein naheliegender Schutz gegen diese Bedrohung ist, dass System- und App-Entwickler:innen Best Practices für Sicherheit und Softwareentwicklung befolgen. Zusätzlich lässt sich die Angriffsfläche verkleinern, z. B. indem die Softwarekomponenten, die sensible Daten verarbeiten, minimiert werden. Um zu verhindern, dass andere Komponenten auf die sensiblen Daten zugreifen, sollten die Isolationsfunktionen und Sandboxes der

mobilen Plattform genutzt werden. Um die Daten noch besser zu schützen, sollten hardwaregestützte Schutzfunktionen verwendet werden. Das gilt insbesondere für kryptografisches Material wie das private Schlüsselmaterial von Identitäten. Dazu wird empfohlen, die Softwarekomponenten des „Key Management System“ (KMS), die dieses kryptografische Material verarbeiten (z. B. um andere Daten damit zu ver-/entschlüsseln oder zu signieren), in isolierte Ausführungsumgebungen zu verlagern, etwa ein Trusted Execution Environment (TEE), ein Secure Element oder ein Hardware Security Module (HSM).

4.2. Mechanismen für gerätegebundene Identitäten

Credentials können üblicherweise aus dem Quellgerät exportiert und in das Zielgerät importiert bzw. dort wiederhergestellt werden, die zugehörigen kryptografischen Schlüssel sind jedoch mitunter gerätegebunden. Die in Abschnitt 4.1 oben beschriebenen hardwarebasierten Isolationsmechanismen bilden die Grundlage für die Speicherung der Identität und lassen sich zugleich zur Umsetzung der Gerätebindung nutzen. Um verschiedene Anwendungsfälle zu unterstützen, gibt es dafür unterschiedliche Möglichkeiten:

- Export aller Daten zulassen: Alle Daten können aus dem sicheren Speicher des Geräts exportiert, gesichert und später auf dem Zielgerät importiert bzw. wiederhergestellt werden. Die Daten sollten vor dem Export dennoch geschützt (d. h. verschlüsselt) werden (siehe Abschnitt 4.3 unten).
- Export jeglicher Daten verhindern: Alle Daten sind an das Gerät gebunden und können nicht exportiert werden. Dies betrifft typischerweise private bzw. sensible Daten, da andere Daten (etwa öffentliche Schlüssel) für die Funktion des Geräts und der Geschäftslogik exportiert werden müssen. Dieser Schutz lässt sich umsetzen, indem die Schnittstelle des sicheren Speichers auf kryptografische Operationen und Importfunktionen beschränkt wird. Dadurch kann andere Software auf dem Gerät (und sogar andere Softwarekomponenten derselben App bzw. desselben Werkzeugs) nicht auf die sensiblen Daten zugreifen und sie daher weder exportieren noch sichern. Auf diese Weise lassen sich rein physische Identitäten umsetzen.
- Export einiger Daten zulassen: Eine Kombination beider Fälle besteht darin, den Export mancher Identitätsdaten einzuschränken und bei anderen Daten zuzulassen. Dies lässt sich umsetzen, indem für die Komponente des sicheren Speichers Export- bzw. Backup-Schnittstellen definiert werden, die Zugriffskontrollmechanismen anwenden und die exportierbaren Daten oder Datentypen einschränken. Werden allen im sicheren Speicher abgelegten Daten Metadaten zu Zugriffsberechtigungen angehängt, ist eine fein abgestufte und flexible Zugriffs- bzw. Exportkontrolle möglich. Das ermöglicht verschiedene Wiederherstellungsarten, wie in Abschnitt 3.1 oben beschrieben.
- Sicherstellen, dass die Wiederherstellung nur für bestimmte (Klassen von) Geräten gestartet werden kann: Eine weitere Option besteht darin, den Export von Daten aus dem sicheren Speicher des Geräts zuzulassen, aber das Gerät einzuschränken, das auf die exportierten Daten zugreifen kann. Das gelingt, indem die Daten vor dem Export geschützt werden, d. h. für den kryptografischen (öffentlichen) Schlüssel des konkreten Zielgeräts verschlüsselt werden. Kombiniert man den Verschlüsselungsprozess mit Key-Attestation-Funktionen (z. B. [1, 2]), kann das Quellgerät überprüfen, dass der verwendete öffentliche Schlüssel zum legitimen Zielgerät gehört, und so sicherstellen, dass nur dieses Gerät die Daten entschlüsseln kann. Ist das konkrete Zielgerät (noch) nicht bekannt, sind fortgeschrittenere Schutzmechanismen erforderlich (siehe Abschnitt 4.3 unten).

4.3. Kryptografische Mechanismen für sicheres Backup und Restore (B&R)

Während hardwaregestützter sicherer Speicher gewährleistet, dass sensible Daten beim Speichern und Verarbeiten auf dem Gerät geschützt sind, lassen sich kryptografische Mechanismen einsetzen, um die Daten zu schützen, während sie vom Backup-und-Restore-System verarbeitet werden, d. h. während sie aus dem Quellgerät exportiert, irgendwo gespeichert und später vom Zielgerät geladen und importiert werden. Dazu werden die Daten selbst mit einer standardmäßigen symmetrischen Verschlüsselung (z. B. AES[3]) verschlüsselt. Dadurch sind die Daten geschützt und können nur von Parteien entschlüsselt werden, die im Besitz dieses symmetrischen Datenverschlüsselungsschlüssels sind. Da symmetrische Kryptosysteme für Ver- und Entschlüsselung denselben Schlüssel benötigen, muss dieser symmetrische Datenverschlüsselungsschlüssel auf sichere Weise vom Quellgerät auf das legitime Zielgerät übertragen werden („Schlüsselmanagementproblem"). Als zusätzliche Herausforderung wird angenommen, dass Quell- und Zielgerät nicht gleichzeitig existieren.

Um diese Herausforderung zu lösen, wird es der Management-Komponente ermöglicht, während des Wiederherstellungsprozesses neuen Geräten Zugriff zu gewähren, ohne dass das Quellgerät sie vorher kennen muss. Dazu wird der Datenverschlüsselungsschlüssel mit einem asymmetrischen Schlüssel der Management-Komponente verschlüsselt (Key Encapsulation Mechanism, KEM). Außerdem wird die Management-Komponente in die Lage versetzt, diesen verschlüsselten Schlüssel später neu zu verschlüsseln, sodass das Zielgerät ihn entschlüsseln kann. Dieser Prozess ist auch in Abbildung 2 dargestellt. In den folgenden Unterabschnitten werden zwei Mechanismen für diesen Prozess besprochen.

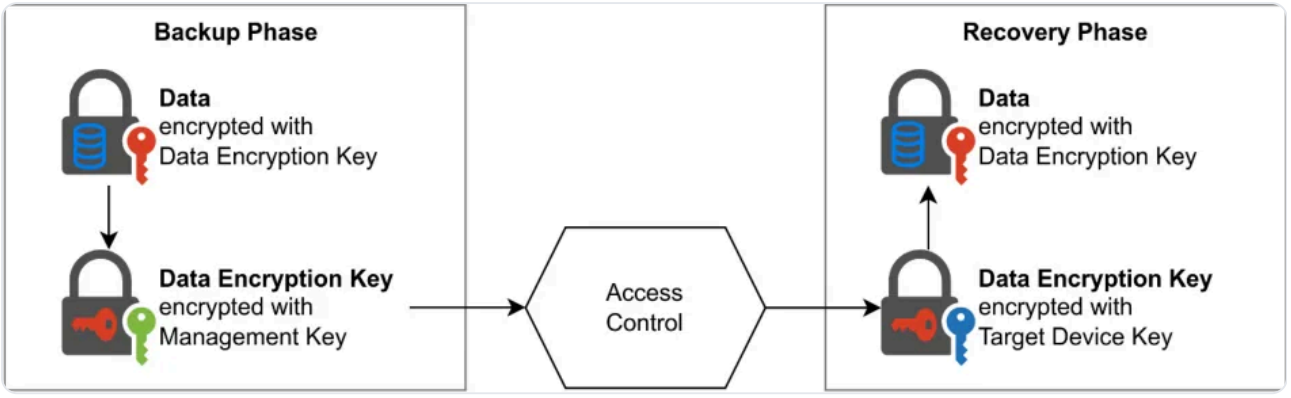


Abbildung 3: Konzeptionelle Darstellung des Zugriffskontrollmechanismus des B&S-Systems

4.3.1. Verwendung asymmetrischer Kryptografie

Um jedem Zielgerät, das in der Backup-Phase noch nicht existiert, Zugriff auf den Datenverschlüsselungsschlüssel der gesicherten Informationen zu gewähren, muss die Management-Komponente den Datenverschlüsselungsschlüssel in der Recovery-Phase für dieses Zielgerät verschlüsseln. Dazu verwendet das Quellgerät den öffentlichen Schlüssel des Managements (und nicht den öffentlichen Schlüssel eines Zielgeräts), um den Datenverschlüsselungsschlüssel zu verschlüsseln. Die Management-Komponente kann den Schlüssel dann entschlüsseln und für das Zielgerät verschlüsseln. Dieser Schritt kann zu einem späteren Zeitpunkt stattfinden (sogar nachdem das Quellgerät nicht mehr verfügbar ist). Dieser Prozess ist auch in Abbildung 4 dargestellt. Dabei kann die Management-Komponente entscheiden, welches Zielgerät auf den Datenverschlüsselungsschlüssel zugreifen (und damit die Daten entschlüsseln und wiederherstellen) darf. In diesem Schritt kann das Management-Gerät auch eine Key

Attestation[4] des Schlüssels des Zielgeräts überprüfen. Dies wird zwar nicht kryptografisch erzwungen, ermöglicht der Management-Komponente aber sicherzustellen, dass sie es mit dem öffentlichen Schlüssel des legitimen Zielgeräts zu tun hat.

Ein wesentlicher Nachteil dieses Ansatzes ist, dass der sensible Datenverschlüsselungsschlüssel entschlüsselt wird, bevor er erneut verschlüsselt wird. Der Schlüssel liegt während des Prozesses also im Klartext vor, entweder bei der Storage-Komponente oder bei der Management-Komponente.

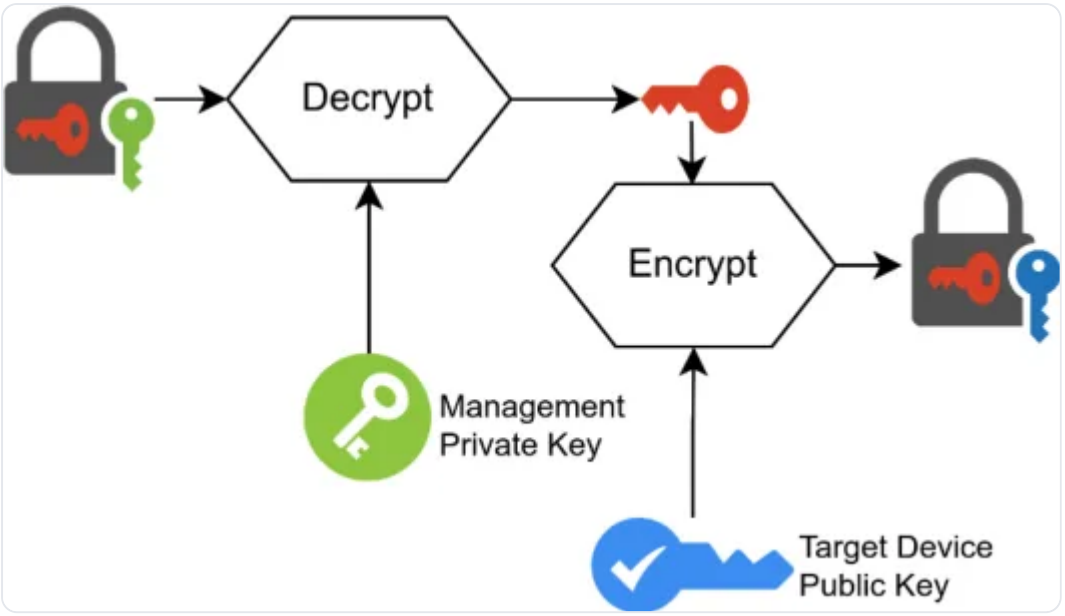


Abbildung 4: B&R-Zugriffskontrolle mit asymmetrischer Kryptografie

4.3.2. Verwendung von Proxy Re-Encryption

Um die Nachteile asymmetrischer Kryptografie in diesem Kontext zu mildern, wird der Einsatz von Proxy Re-Encryption (PRE) vorgeschlagen. Mit PRE kombiniert die Management-Komponente ihren (privaten) Schlüssel und den (öffentlichen) Schlüssel des Zielgeräts zu einem Re-Encryption-Schlüssel. Die Storage-Komponente oder das Zielgerät selbst kann diesen Re-Encryption-Schlüssel dann verwenden, um den eingewickelten bzw. verschlüsselten Datenverschlüsselungsschlüssel so neu zu verschlüsseln, dass er anschließend mit dem eigenen (privaten) Schlüssel entschlüsselt werden kann. Dieser Prozess ist in Abbildung 5 dargestellt. Dabei hat die Storage-Komponente nie Zugriff auf den Datenverschlüsselungsschlüssel im Klartext und kann daher nie auf die Daten zugreifen bzw. sie entschlüsseln. Diese Methode ermöglicht außerdem einen asynchroneren Wiederherstellungsprozess, da das Management-Gerät den Re-Encryption-Schlüssel (und damit den Zugriff des Zielgeräts) jederzeit erzeugen kann und überhaupt nicht mit der Storage-Komponente kommunizieren muss.

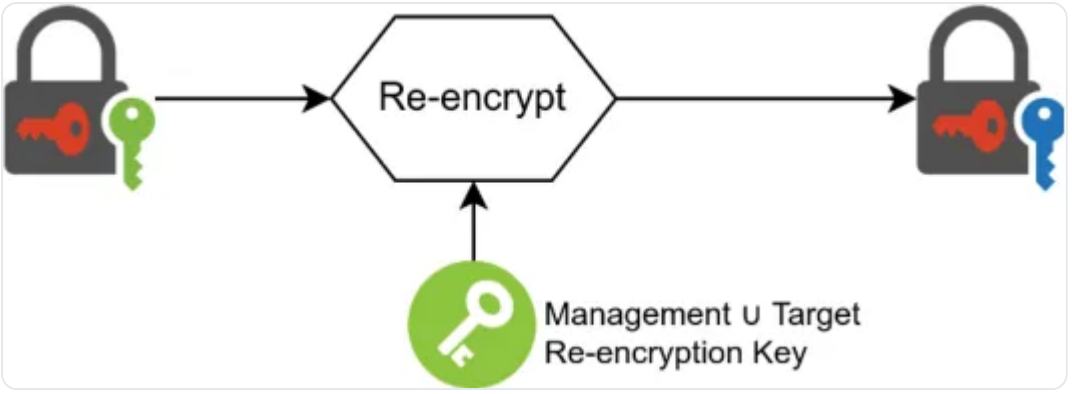


Abbildung 5: B&R-Zugriffskontrolle mit Proxy Re-Encryption

5. Prototypdesign

Um die Praxistauglichkeit des Designs des Backup-und-Recovery-Systems zu demonstrieren, wird die oben beschriebene Architektur instanziiert. Um den Zugriffskontrollaspekt des Recovery-Systems zu ermöglichen, wird Proxy Re-Encryption eingesetzt. Dadurch kann die Management-Komponente den Zugriff auf die Daten steuern und neuen (Ziel-)Geräten Zugriff gewähren, während die Storage-Komponente keinen Zugriff auf die Daten hat. Dies ist ein Vorteil gegenüber einfacher asymmetrischer Kryptografie, bei der die Storage-Komponente die Daten entschlüsseln müsste, um sie dann für das Zielgerät zu verschlüsseln. Um den hardwaregestützten Schutz der auf dem Gerät gespeicherten Daten beizubehalten, wird der B&R-Client auf dem Gerät mit einem Datenschutz auf Basis eines Trusted Execution Environment (TEE) [3, 4] kombiniert. Dadurch lässt sich sicherstellen, dass die Daten in der Secure World bereits für die Zielumgebung verschlüsselt sind und somit vor möglicher auf dem Gerät vorhandener Malware geschützt werden. Dieses Prototypdesign mit TEE und zwei IOT-Geräten ist in Abbildung 6 unten dargestellt.

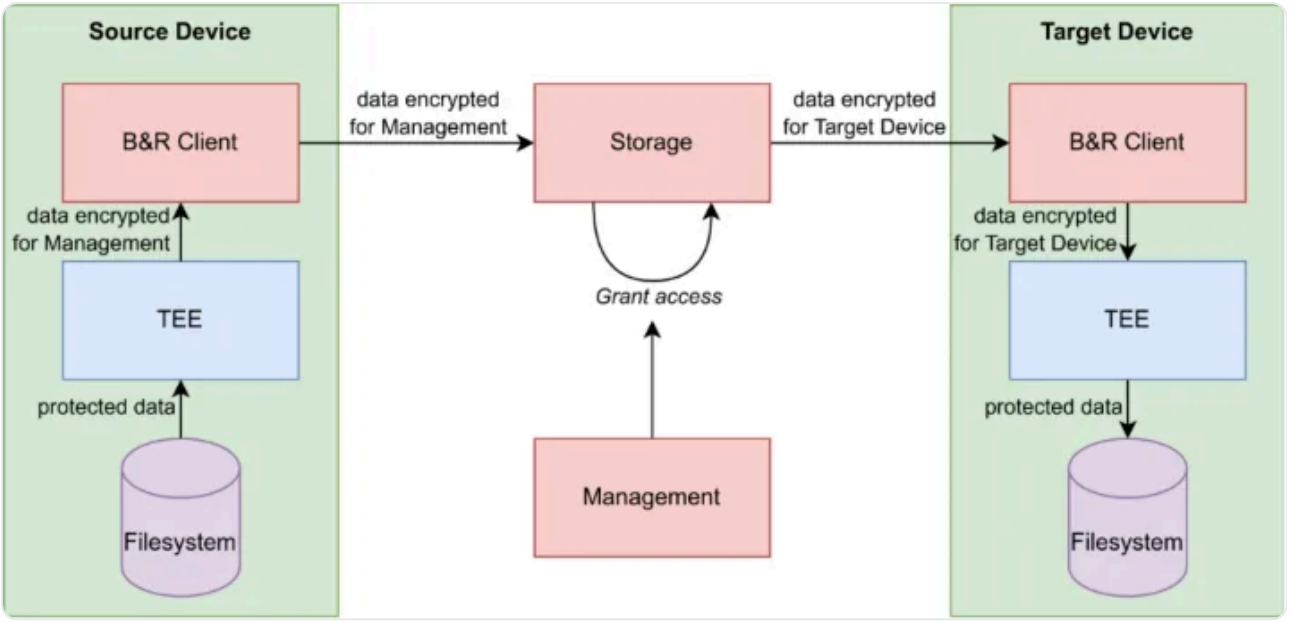


Abbildung 6: Konzeptioneller Überblick über die B&R-Prototypimplementierung

6. Fazit

In diesem Bericht wurde das Thema Identitätswiederherstellung im Kontext mobiler Identitäts-Wallets und smarter bzw. IOT-Geräte behandelt. Im Einzelnen lag der Fokus auf Anwendungen, die hardwaregeschützten Speicher für Identitätsdaten nutzen, aber dennoch eine Wiederherstellung bei Geräteverlust oder -ausfall ermöglichen wollen. Es wurden die verschiedenen Arten von Identitätsinformationen (physisch vs. logisch) und Wiederherstellungsprozesse (Backup und Restore von Identitätsinformationen, erneutes Enrollment) hervorgehoben. Damit die Daten auf dem Gerät sowie während des Wiederherstellungsprozesses geschützt sind, wurden technische Aspekte sicherer Speicherung und kryptografische Mechanismen für eine flexible Zugriffskontrolle bei der Wiederherstellung besprochen. Empfohlen wurden hierbei hardwaregestützte Speichermechanismen und asymmetrische Kryptografie sowie Proxy Re-Encryption. Der Bericht schließt mit einem technischen Prototyp der besprochenen Wiederherstellungsprozesse.

Referenzen

[1] Prünster, B, Palfinger, G & Kollmann, CP. 2019, Fides – Unleashing the Full Potential of Remote Attestation. in Proceedings of the 16th International Joint Conference on e-Business and Telecommunications: SECRYPT, SciTePress. https://doi.org/10.5220/0008121003140321

[2] Czerny, R, Kollmann, CP, Podgorelec, B, Prünster, B & Zefferer, T. 2023, Smoothing the Ride: Providing a Seamless Upgrade Path from Established Cross-Border eID Workflows Towards eID Wallet Systems. in Proceedings of the 20th International Conference on Security and Cryptography, SciTePress. https://doi.org/10.5220/0012091900003555

[3] GlobalPlatform Consortium. 2021, TEE Internal Core API Specification v1.3.1. https://globalplatform.org/specs-library/tee-internal-core-api-specification/

[4] Göttel, C., Felber, P., & Schiavoni, V. 2019, Developing secure services for IoT with OP-TEE: a first look at performance and usability. In Distributed Applications and Interoperable Systems: 19th IFIP WG 6.1 International Conference, DAIS 2019, Held as Part of the 14th International Federated Conference on Distributed Computing Techniques, DisCoTec 2019. Springer International Publishing

1. https://developer.android.com/privacy-and-security/keystore ↩
2. https://datatracker.ietf.org/doc/html/rfc7800 ↩
3. https://csrc.nist.gov/pubs/fips/197/final ↩
4. https://a-sit-plus.github.io/attestation-service ↩