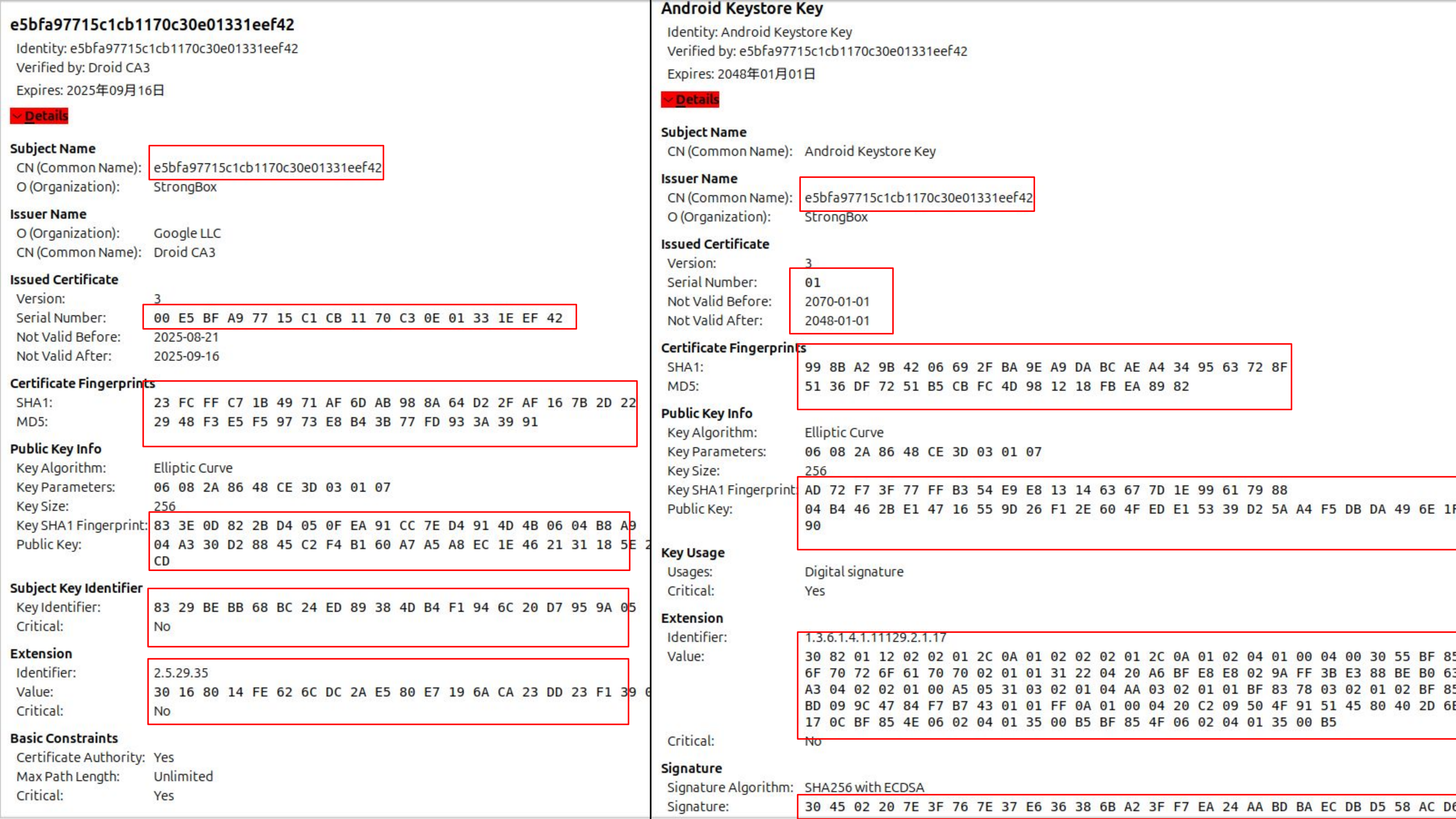
Anastasia

Cinderella's Stepsister Turning Shabby X.509 Certificates into Elegant Anonymous Device Attestations with the Magic of Noir

Problem

- X.509 chains leak serials, pubkeys, signatures
- Enables tracking & linkability
- Still widely adopted in services & protocols
- Android Key Attestation relies on X.509
  → systemic privacy risk



e5bfa97715c1cb1170c30e01331eef42

Identity: e5bfa97715c1cb1170c30e01331eef42
Verified by: Droid CA3
Expires: 2025年09月16日

Subject Name

CN (Common Name): e5bfa97715c1cb1170c30e01331eef42
O (Organization): StrongBox

Issuer Name

O (Organization): Google LLC
CN (Common Name): Droid CA3

Issued Certificate

Version: 3
Serial Number: 00 E5 BF A9 77 15 C1 CB 11 70 C3 0E 01 33 1E EF 42
Not Valid Before: 2025-08-21
Not Valid After: 2025-09-16

Certificate Fingerprints

SHA1: 23 FC FF C7 1B 49 71 AF 6D AB 98 8A 64 D2 2F AF 16 7B 2D 22
MD5: 29 48 F3 E5 F5 97 73 E8 B4 3B 77 FD 93 3A 39 91

Public Key Info

Key Algorithm: Elliptic Curve
Key Parameters: 06 08 2A 86 48 CE 3D 03 01 07
Key Size: 256
Key SHA1 Fingerprint: 83 3E 0D 82 2B D4 05 0F EA 91 CC 7E D4 91 4D 4B 06 04 B8 A9
Public Key: 04 A3 30 D2 88 45 C2 F4 B1 60 A7 A5 A8 EC 1E 46 21 31 18 5E 2
CD

Subject Key Identifier

Key Identifier: 83 29 BE BB 68 BC 24 ED 89 38 4D B4 F1 94 6C 20 D7 95 9A 05
Critical: No

Extension

Identifier: 2.5.29.35
Value: 30 16 80 14 FE 62 6C DC 2A E5 80 E7 19 6A CA 23 DD 23 F1 39 0
Critical: No

Basic Constraints

Certificate Authority: Yes
Max Path Length: Unlimited
Critical: Yes

Android Keystore Key

Identity: Android Keystore Key
Verified by: e5bfa97715c1cb1170c30e01331eef42
Expires: 2048年01月01日

Subject Name

CN (Common Name): Android Keystore Key

Issuer Name

CN (Common Name): e5bfa97715c1cb1170c30e01331eef42
O (Organization): StrongBox

Issued Certificate

Version: 3
Serial Number: 01
Not Valid Before: 2070-01-01
Not Valid After: 2048-01-01

Certificate Fingerprints

SHA1: 99 8B A2 9B 42 06 69 2F BA 9E A9 DA BC AE A4 34 95 63 72 8F
MD5: 51 36 DF 72 51 B5 CB FC 4D 98 12 18 FB EA 89 82

Public Key Info

Key Algorithm: Elliptic Curve
Key Parameters: 06 08 2A 86 48 CE 3D 03 01 07
Key Size: 256
Key SHA1 Fingerprint: AD 72 F7 3F 77 FF B3 54 E9 E8 13 14 63 67 7D 1E 99 61 79 88
Public Key: 04 B4 46 2B E1 47 16 55 9D 26 F1 2E 60 4F ED E1 53 39 D2 5A A4 F5 DB DA 49 6E 1F
90

Key Usage

Usages: Digital signature
Critical: Yes

Extension

Identifier: 1.3.6.1.4.1.11129.2.1.17
Value:
```
30 82 01 12 02 02 01 2C 0A 01 02 02 02 01 2C 0A 01 02 04 01 00 04 00 30 55 BF 85
6F 70 72 6F 61 70 70 02 01 01 31 22 04 20 A6 BF E8 E8 02 9A FF 3B E3 88 BE B0 63
A3 04 02 02 01 00 A5 05 31 03 02 01 04 AA 03 02 01 01 BF 83 78 03 02 01 02 BF 85
BD 09 9C 47 84 F7 B7 43 01 01 FF 0A 01 00 04 20 C2 09 50 4F 91 51 45 80 40 2D 6E
17 0C BF 85 4E 06 02 04 01 35 00 B5 BF 85 4F 06 02 04 01 35 00 B5
```
Critical: No

Signature

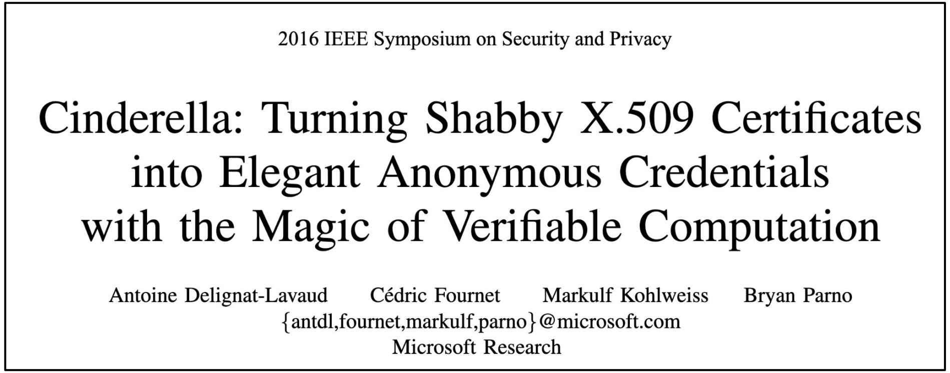
Signature Algorithm: SHA256 with ECDSA
Signature: 30 45 02 20 7E 3F 76 7E 37 E6 36 38 6B A2 3F F7 EA 24 AA BD BA EC DB D5 58 AC D6

Prior Work: Cinderella (IEEE S&P 2016)

- Use zk-SNARKs (Pinocchio) for RSA-based X.509
- ✅ Tiny proofs (288B), fast verification (ms)
- ✅ *Parse outside, re-serialize inside circuit*
- ❌ (non-universal) Trusted Setup, GB params
- ❌ Proof gen

  = **tens of seconds**

  → not for mobile



2016 IEEE Symposium on Security and Privacy

Cinderella: Turning Shabby X.509 Certificates into Elegant Anonymous Credentials with the Magic of Verifiable Computation

Antoine Delignat-Lavaud Cédric Fournet Markulf Kohlweiss Bryan Parno
{antdl,fournet,markulf,parno}@microsoft.com
Microsoft Research

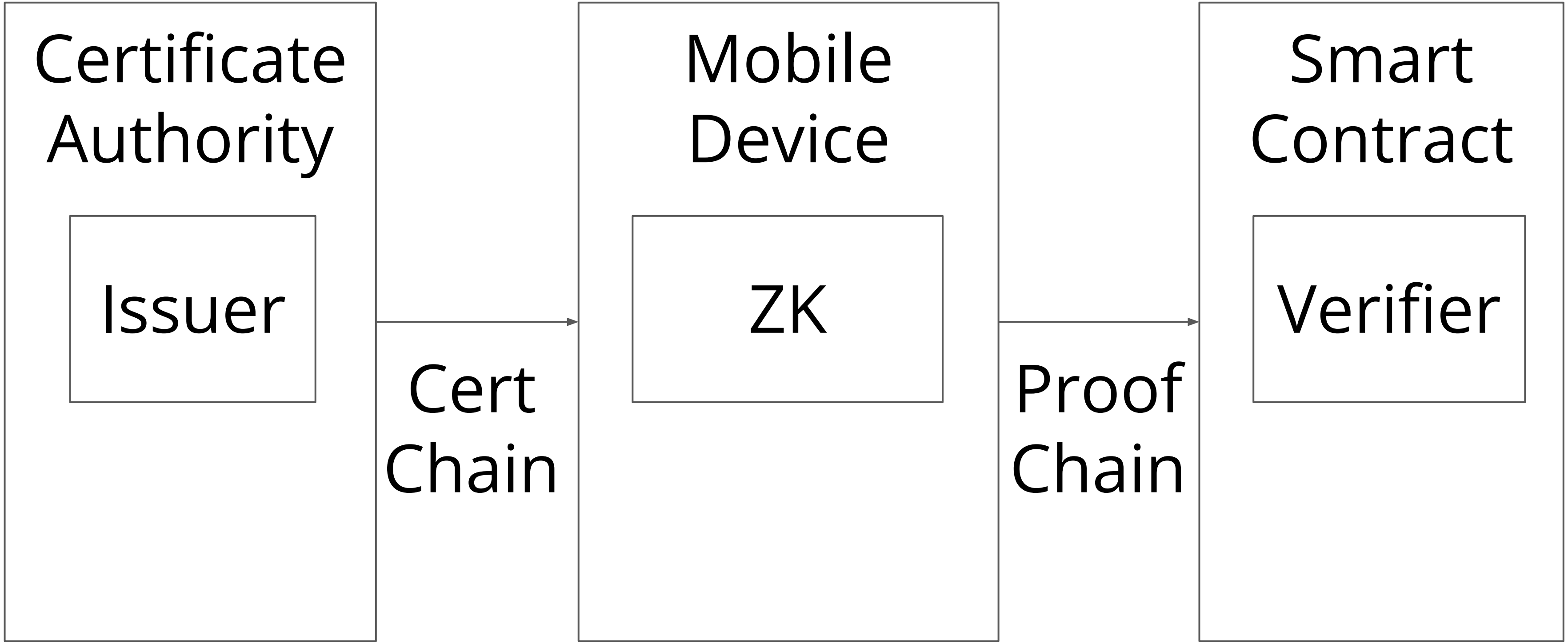
Anastasia

Cinderella's Stepsister Turning Shabby X.509 Certificates into Elegant Anonymous **Device Attestations** with the Magic of **Noir**

Our Solution: Anastasia

- UltraHonk (Highly Optimized Plonk-style ZKP)
- Circuits in Noir DSL (instead of C)
- Support ECDSA (for Android Key Attestations)
- Split-proof approach → memory friendly
- Rust lib + Kotlin SDK (powered by Mopro)
- Verifier as a Solidity contract

Architecture



Certificate Authority

Issuer

Cert Chain

Mobile Device

ZK

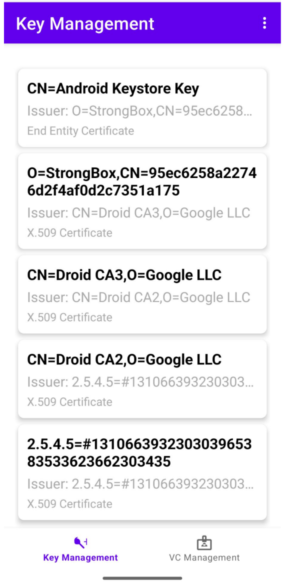
Proof Chain

Smart Contract

Verifier

Live Demo (Android device)

1. Generate a key pair and X.509 cert chain in Secure Element
2. Prove with Noir (2-cert chain)
3. Verify proof in Solidity contract



Key Management

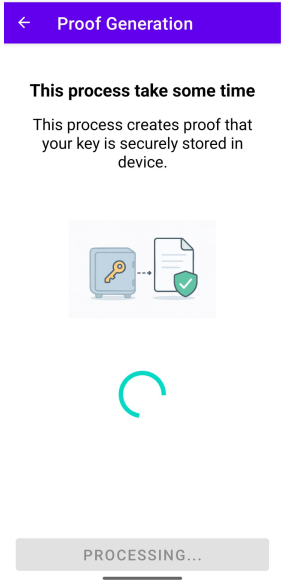
CN=Android Keystore Key
Issuer: O=StrongBox,CN=95ec6258...
End Entity Certificate

O=StrongBox,CN=95ec6258a2274 6d2f4af0d2c7351a175
Issuer: CN=Droid CA3,O=Google LLC
X.509 Certificate

CN=Droid CA3,O=Google LLC
Issuer: CN=Droid CA2,O=Google LLC
X.509 Certificate

CN=Droid CA2,O=Google LLC
Issuer: 2.5.4.5=#131066393230303...
X.509 Certificate

2.5.4.5=#1310663932303039653 835336236623034 35
Issuer: 2.5.4.5=#131066393230303...
X.509 Certificate



Proof Generation

This process take some time

This process creates proof that your key is securely stored in device.

Current Limitations

- Only 2 certs (full = 5 certs)
- Proof gen: **>20s** on Google Pixel 9a
- Solidity verifier gas-heavy
- No revocation (CRL/OCSP)
- iOS not yet supported
- No formal security audit yet

Future Potential

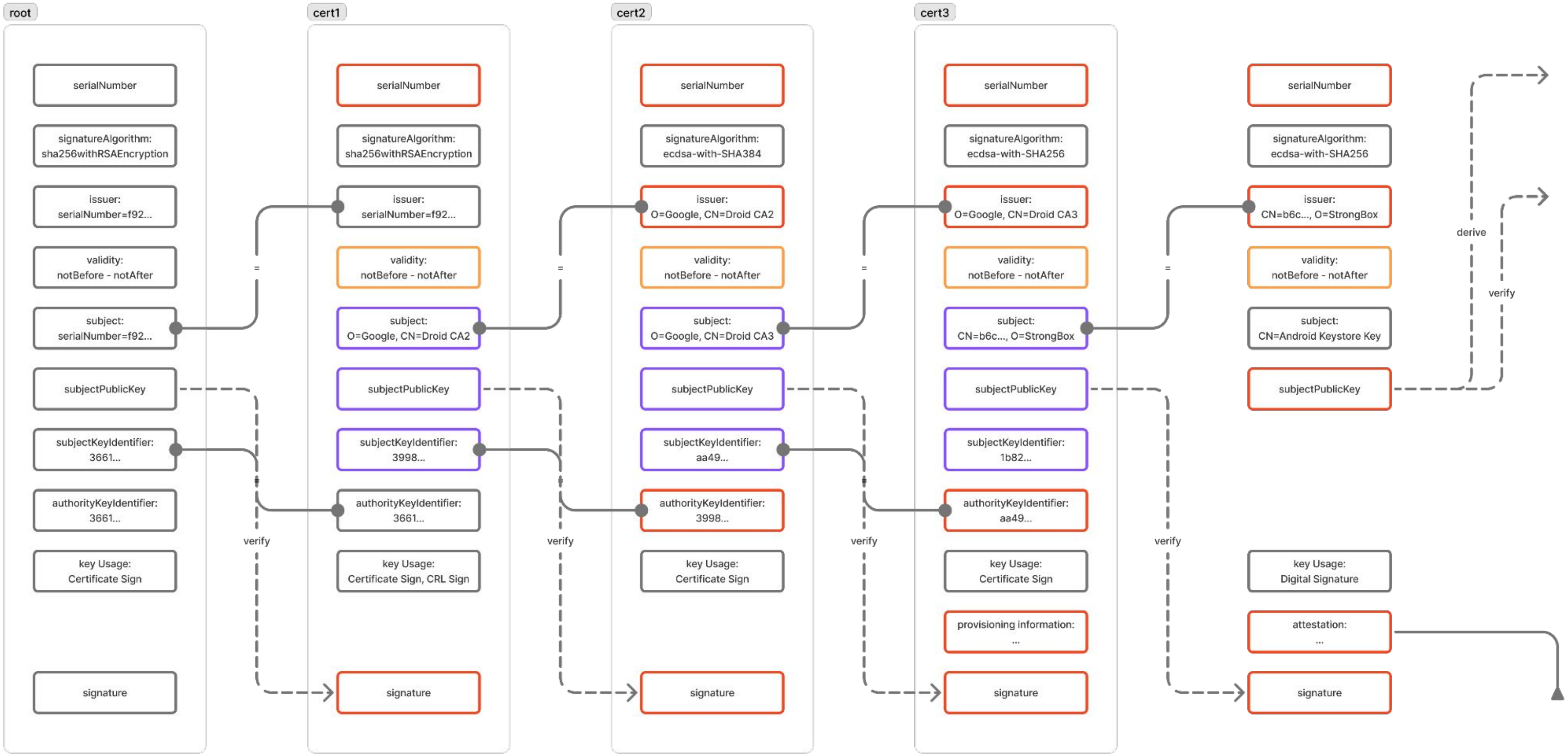
- Real integration with Digital Identity Wallets
- Device-attested keys as pseudonyms
- Lighter verifier contracts
- Cross-platform (Android + iOS)
- Beyond device attestations:
  - Anonymization of user-issued X.509 certs
  - Issuer-hiding credentials
  - General anonymous PKI proofs

Links

- This slides
- Repository

- Cinderella Paper
- Cinderella Slides

Certificate Chain



root	cert1	cert2	cert3	
serialNumber	serialNumber	serialNumber	serialNumber	serialNumber
signatureAlgorithm: sha256withRSAEncryption	signatureAlgorithm: sha256withRSAEncryption	signatureAlgorithm: ecdsa-with-SHA384	signatureAlgorithm: ecdsa-with-SHA256	signatureAlgorithm: ecdsa-with-SHA256
issuer: serialNumber=f92...	issuer: serialNumber=f92...	issuer: O=Google, CN=Droid CA2	issuer: O=Google, CN=Droid CA3	issuer: CN=b6c..., O=StrongBox
validity: notBefore - notAfter	validity: notBefore - notAfter	validity: notBefore - notAfter	validity: notBefore - notAfter	validity: notBefore - notAfter
subject: serialNumber=f92...	subject: O=Google, CN=Droid CA2	subject: O=Google, CN=Droid CA3	subject: CN=b6c..., O=StrongBox	subject: CN=Android Keystore Key
subjectPublicKey	subjectPublicKey	subjectPublicKey	subjectPublicKey	subjectPublicKey
subjectKeyIdentifier: 3661...	subjectKeyIdentifier: 3998...	subjectKeyIdentifier: aa49...	subjectKeyIdentifier: 1b82...	
authorityKeyIdentifier: 3661...	authorityKeyIdentifier: 3661...	authorityKeyIdentifier: 3998...	authorityKeyIdentifier: aa49...	
key Usage: Certificate Sign	key Usage: Certificate Sign, CRL Sign	key Usage: Certificate Sign	key Usage: Certificate Sign	key Usage: Digital Signature
			provisioning information: ...	attestation: ...
signature	signature	signature	signature	signature