Secure Systems Group, Aalto University

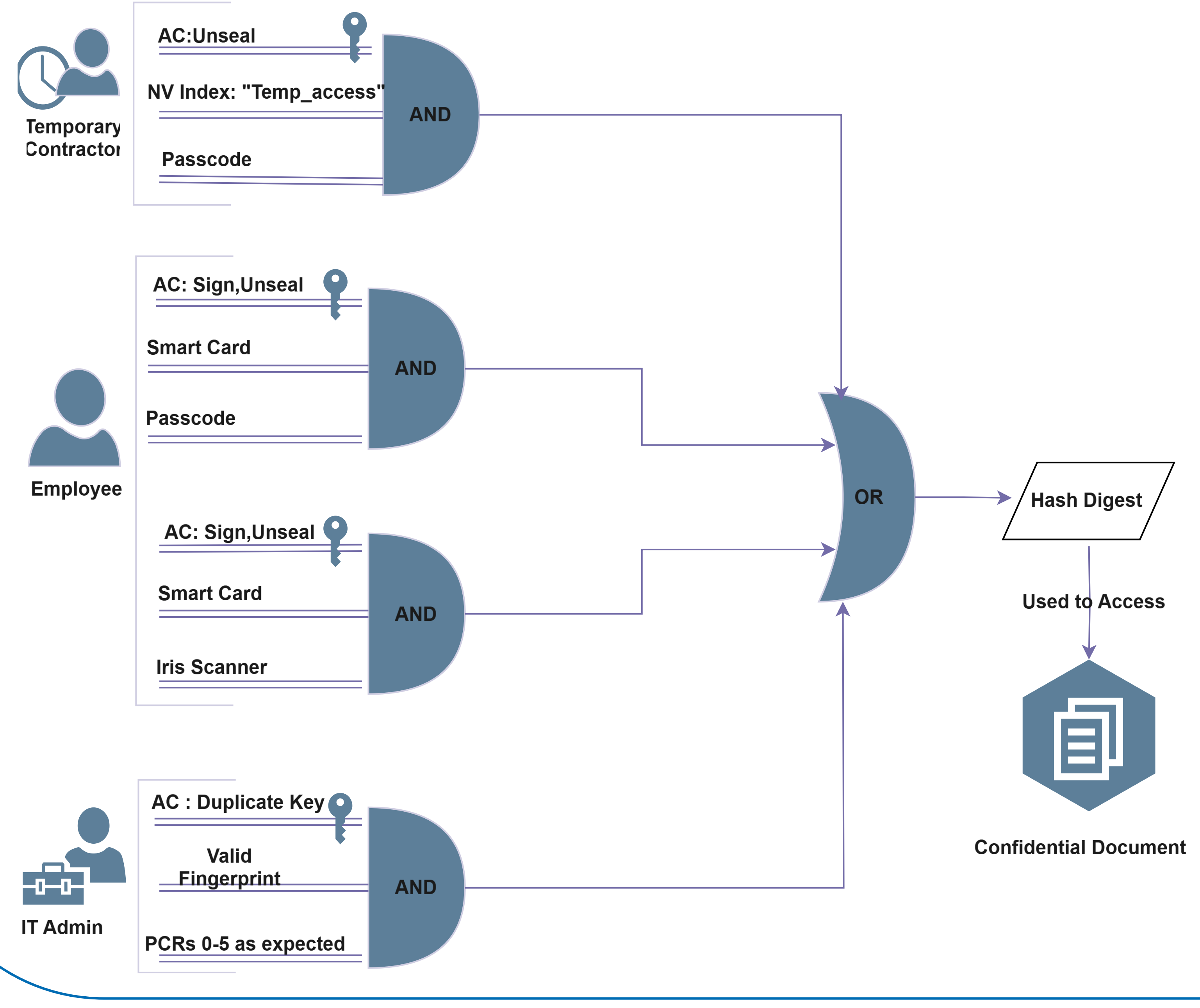
Making TPM Extended Authorization Practical

Mostafa Ghozal , Lachlan Gunn

What is TPM ?

Trusted Platform Module (TPM) is a tamper-resistant hardware-based crypto-processor that performs platform integrity checks, key management & sealing, attestation to third parties.

Enhanced Authorization (EA)



- Defines complex policies that control TPM protected operations.
- Tree of logical assertions including PCRs, commands, AC and Boolean logic.
- Result is a SHA-256 hash, stored in the TPM.
- EA remains under-utilized due to their complexity, opaque digests and lack of tooling for debugging and understanding policies

TPM ARCHITECT

BUILD, UNDERSTAND, DEBUG & MANAGE TPM 2.0 POLICIES

1. User inputs the policy using a readable DSL by CLI or Interactive Web App GUI

```
(PolicyAuthValue OR PolicyPCR(--alg sha256 --pcrs 0:abc,1:def)) AND PolicyCommandCode(Sign)
```

2. The tool visualizes the policy building process in a tree of command chains and digests
3. Developers can debug the policy generation steps and modify in the policy
4. Exports the following:

Digest Binary File
Applies the policy directly on TPM2Tools

Bash Script
Rebuilds the policy's steps on TPM2Tools

Log File
Digest Computation Trace

5. Log files can be loaded to the tool to reload the policy and modify it in the future

Implementation: Built as modular rust library, providing both a CLI interface and WASM-based React web app

Aalto University