The FutureTPM project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 779391.

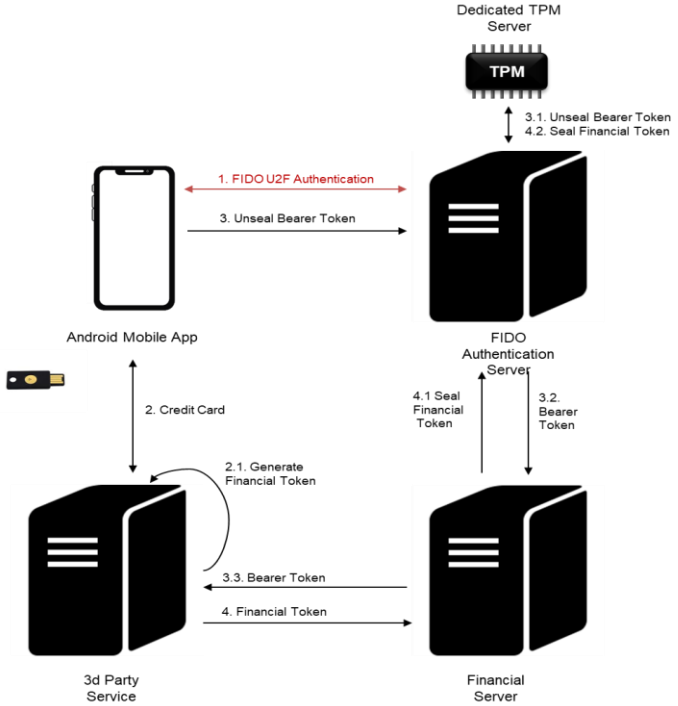
FutureTPM H2020 PROJECT: WP6 -Secure Mobile Wallet and Payments

Final Review Meeting, Feb 18, 2021, Virtual

Dr. Dimitris Papamartzivanos, UBITECH
Joined work with INDEV

Secure Mobile Wallet and Payments - Overview

- Mobile wallet and e-Payment have become and important complement to traditional payment means.
- The number of financial transactions executed in one-touch manner have led to a tremendous amount of financial data that pose strong security, privacy and trust requirements.



Why we need FutureTPM?

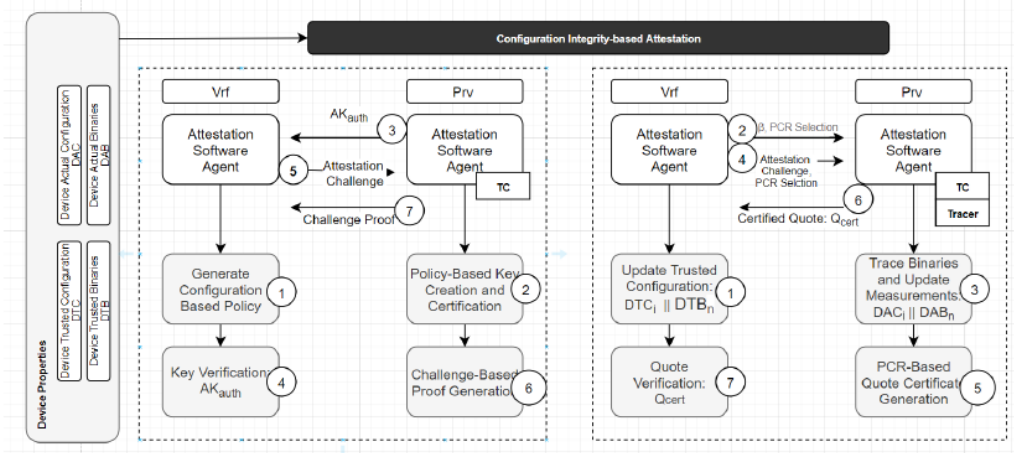
- Current status:
  - Implementation gaps and the extended attack surface of mobile devices increase the cyber risk.
  - Design gap: No use of Trust computing
  - No protection against QR attacks

- QR TPM: Enhance the security posture the domain by providing:
  - Security and trust guarantees at the device level for sensitive financial data and transaction enablers (i.e., authentication and financial tokens)
  - Operational assurance of the mobile device and running applications
    - Configuration Integrity Verification through Remote Attestation
  - Privacy and trust guarantees for protecting users' identity in a verifiable manner
    - Direct Anonymous Attestation

Functionalities of the user stories

- Secure management of tokens
  - Sealing and unsealing of sensitive authentication and financial tokens in the TPM

- Attestation schemes for operational assurance:
  - Attestation by Quote
  - Attestation by Proof



1st Experimental Phase

- **Functionalities**: Sealing, Unsealing, Key Generation
- Integration with Software QR TPM using Kyber algorithm
- Testing and evaluation based on KPIs on a round of tests using HW TPM2.0 and SW QR TPM
  - At Application Level
  - At TSS Level

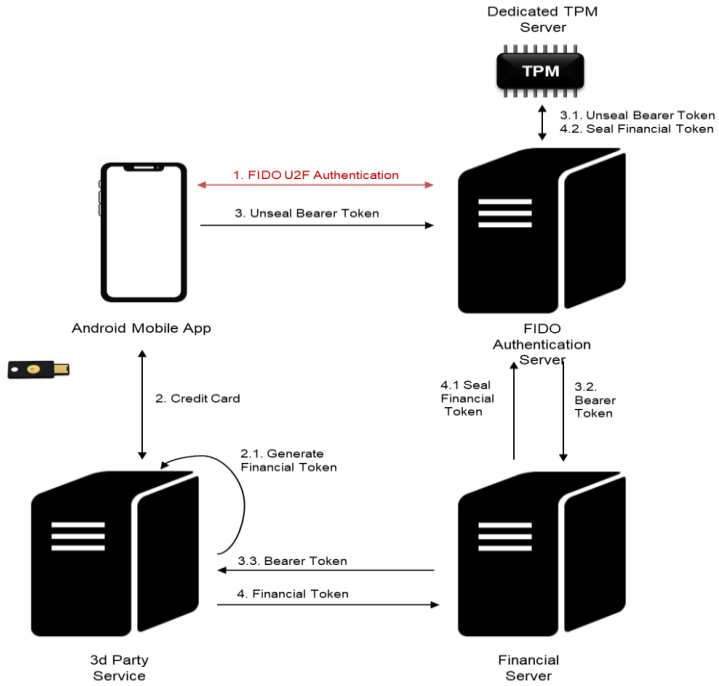
Implementation Path

- Successful Integration of the FIDO U2F authentication protocol in the use case workflow
- Sealing, Unsealing and Key Generation functionalities using Kyber in the SW QR TPM
- The TPM-based functionalities met the KPIs
- FIDO Registration and Authentication met the KPIs

Results and Challenges Faced

User stories: 1st Experimental Period

- **INDEV.AU.1** - As an Individual User I want to log in to the INDEV Service and keep safe the bearer token.
- **INDEV.AU.2** - As an Individual User I want to use an external service to generate tokens for my credit card that go directly in the TPM and avoid revealing my credit card to the server.
- Using HW TPM2.0 and SW QR TPM (D6.3)



2nd Experimental Phase

- **Functionalities**: Sealing, Unsealing, Key Generation, Attestation by Quote, Attestation by Proof
- Integration with Hardware QR TPM using NewHope and BLISS QR algorithms
- Testing and evaluation based on KPIs on a round of tests using HW QR TPM
  - At Application Level
  - At TSS Level
  - At Network Level

Implementation Path

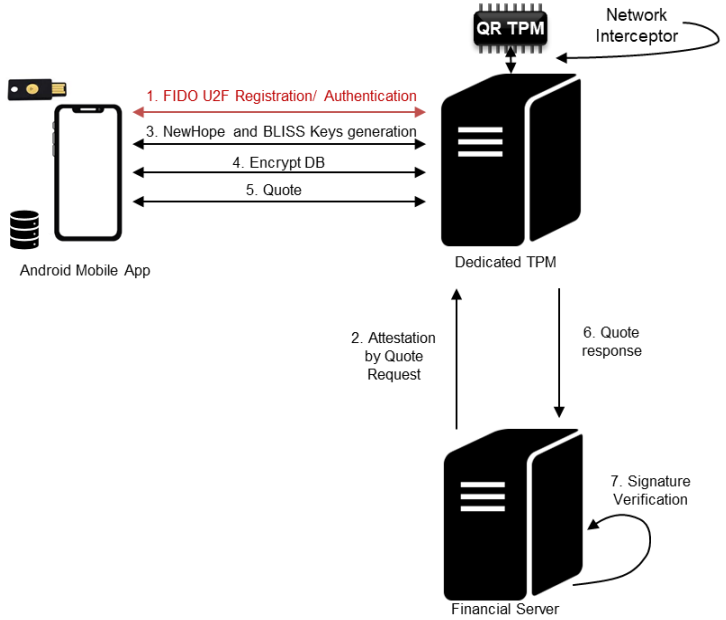
- Successful integration of the HW QR TPM in the use case
- Modification of eBPF tracer to capture and measure TPM commands at the network level.
- Realization and evaluation of Attestation by Quote and Attestation by Proof schemes using the HW QR TPM
- Attestation schemes met the KPIs
- BLISS key generation introduced delay given the current implementation of the HW QR TPM.

Results and Challenges Faced

User stories: 2nd Experimental Period

- **INDEV.AU.3** - As an Individual User I want to ensure that my financial transactions history is secure and not tampered with

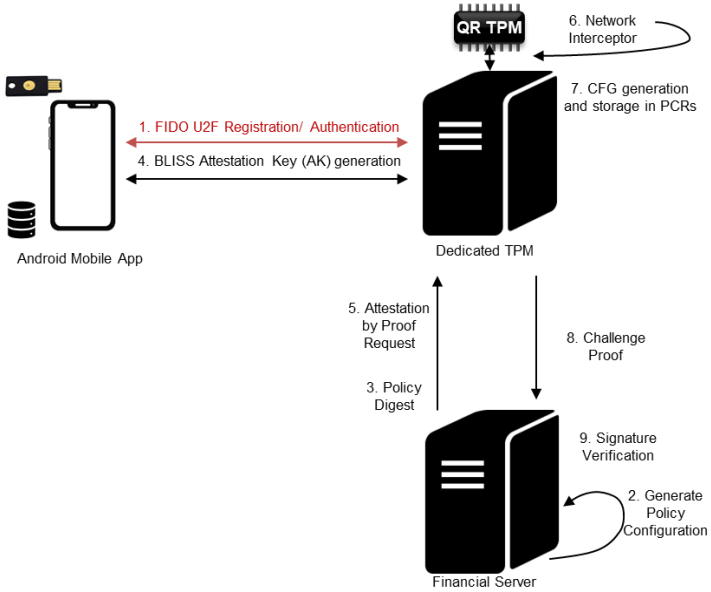
- Attestation by Quote using BLISS
- Database encryption using NewHope



User stories: 2nd Experimental Period

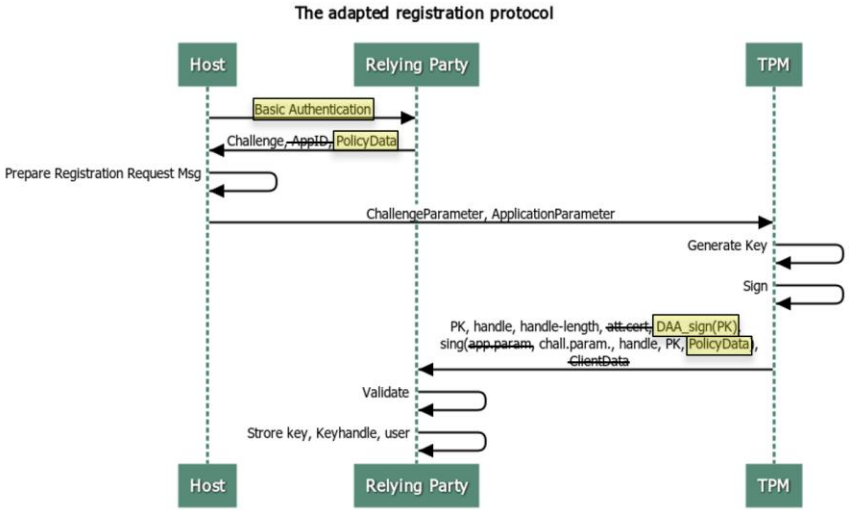
- **INDEV.AU.4** - As an Individual User I want to verify the integrity of the systemic environment setup of the device used to connect to the service

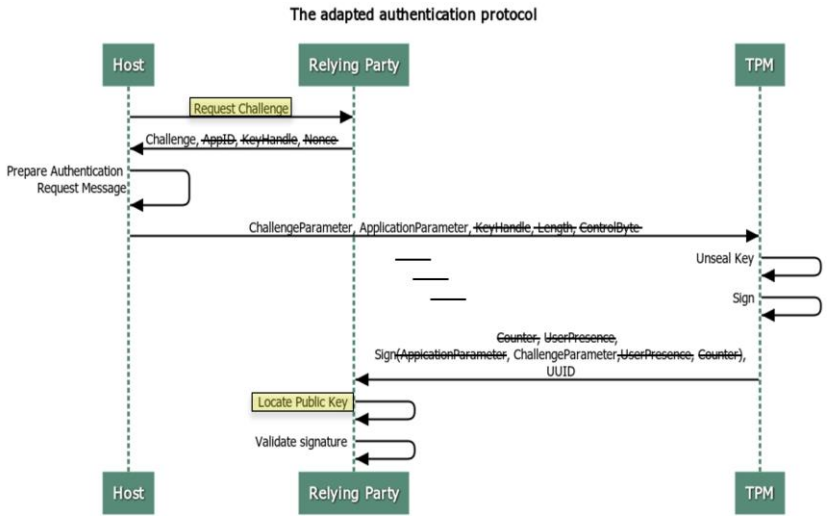
- Attestation by Proof using BLISS



User stories: 2nd Experimental Period

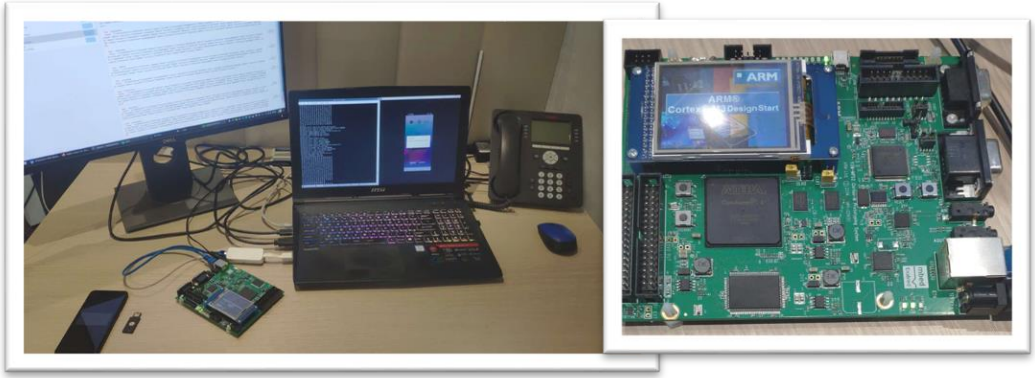
- **INDEV.AU.5** - As an Individual User I want to perform the two-factor authentication with the Financial service through the TPM

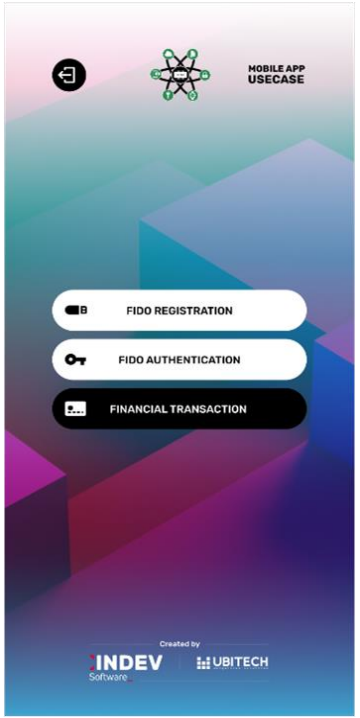




Demonstration and lab setup

- Application functionalities
  - FIDO Registration (Sealing)
  - FIDO Authentication (Unsealing)
  - Execute financial transaction (Attestation by Quote)
  - On demand Integrity verification (Attestation By Proof)





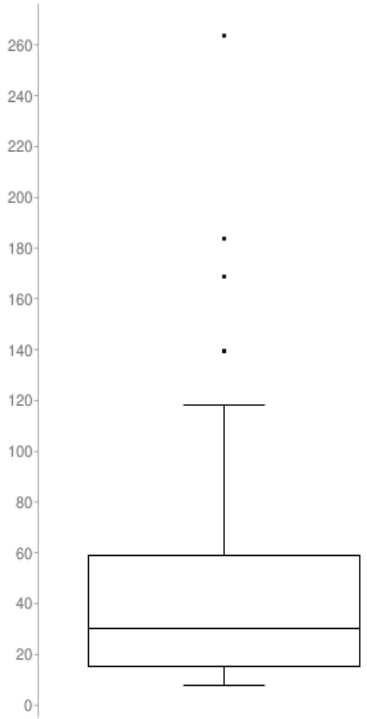
QR Algorithms: Performance of basic functions

ms	Key Creation	Signature	Verify Signature	Encryption	Decryption
NewHope	781,62	---	----	763.23	765.04
BLISS	40242.62	1535.49	601.12	---	---

QR Algorithms: Performance of basic functions

- A closer look on BLISS performance on HW QR TPM

CC_Create (BLISS) statistics	
Max	263.54 seconds
Min	7.94 seconds
Range	255.6 seconds
St. Deviation	42.63 seconds
Coefficient	0.9822



Quantitative KPIs

ID	Metric	Target Value	Acceptance criteria	Mandatory / Good to Have / Optional	Measured by M24 and M36	Comments
1	Amount of **sealed objects**	>=2	=2	M	With TPM2.0: **100%** With FutureTPM: **100%**	**Target Achieved**. Successfully sealed both Bearer and Financial Tokens.
2	Performance of **sealing** functionality within the domain of ms	<=1000 ms	<=2000 ms	M	With TPM2.0: **306.48 ms** With SW FutureTPM: **1027.21 ms** With HW FutureTPM: **1024.00 ms**	**Target Achieved.** The sealing performance is below the acceptance threshold. Using either the SW or the HW implementation of the FutureTPM
3	Performance of the **FIDO Registration**	<=2 sec	<=3 sec	M	With TPM2.0: **0.063 ms** With FutureTPM: **0.063 ms**	**Target achieved.** We consider only the server-side processes for user registration, excluding network latency and user's interaction with the U2F Security Key. Target achieved.
4	Performance of **the FIDO Authentication**	<=1.5 sec	<=2 sec	M	With TPM2.0: **0.0038 ms** With FutureTPM: **0.0038 ms**	**Target achieved.** We consider only the server-side processes for authentication, excluding network latency and user's interaction with the U2F Security Key. Target achieved.
5	Performance of the control flow property-based **attestation** toolkit for the operational correctness	<=7 sec	<=10 sec	M	With HW FutureTPM: **Attes.By.Quote** [CC_Quote + CC_VerifySignature] = 3.59 sec **Attes.By.Proof** [CC_Sign + CC_VerifySignature] = **3.55 secs**	**Target achieved**. For this KPI we consider the time needed to perform the core attestation by Quote of Proof schemes. That is we sum the timings of CC_Quote, CC_Sign and CC_VerifySignature, as shown in the previous column. The attestation key creation is addressed by the following KPI.
6	Performance of **key generation** functionality within the domain of ms	<=20 ms	<=30 ms	M	With HW FutureTPM: **NewHope**: 780 ms **BLISS**: 43405 ms	The timings given here for the key creation of NewHope and BLISS represent **the average of 100 executions** of the corresponding command. In addition, we report here the timings captured from the network perspective as the closest point to HW TPM that gives the most accurate result.

Qualitative KPIs

ID	Metric	Target Value	Mandatory / Good to Have / Optional	Measured by M24 and M36	Comments
1	Protection of sensitive tokens	Supported	M	With TPM2.0: Yes With FutureTPM: Yes	Successfully sealed both Bearer and Financial Tokens.
2	Confidentiality of local history logs	Supported	M	With FutureTPM: Yes, using NewHope QR scheme	Successfully performed the encryption and decryption commands of NewHope
3	Integrity of local history logs	Supported	M	With FutureTPM: Yes, using BLISS QR scheme to enable the attestation by Quote method.	Successfully performed the integrity verification of the history logs through attestation by Quote and the use of BLISS signature scheme.
4	User authentication through the use of TPM	Supported	M	Target Achieved Documentation is given in Section 2.1.3.	We approached this KPI as a research topic and we developed the required trust models in order to achieve user authentication through the use of TPM and DAA protocol. The evaluation is given in Section 2.1.3.
5	The creation of a TPM-based wallet that can support TPM migration functionality throughout the user's devices	Supported	O	Not implemented. Left for future work as a crucial function for future applications also outside of the fintech scope.	

Discussion

- **Feasibility** and **applicability** of enhanced solutions based on the use of decentralized trust anchors towards future proofing the Fintech supply chain
- **Efficiency** and **scalability** even with the enactment of QR crypto primitives
  - Enhanced privacy can be offered through the (L-)DAA specifications adopted by the FIDO Authentication standards
- **Progressing the state-of-the-art towards new breed of remote attestation algorithms:**
  - Zero touch Configuration Integrity Verification & Control-flow Attestation
  - *Lightweight and real-time tracing can be achieved through software solutions*
- Main hurdle to still overcome - ***Support of HW-based roots-of-trust in mobile devices***
- FutureTPM integration to Fintech application domain as a first step to also consider such advanced solutions in other emerging ecosystems with strict security and privacy requirements

FutureTPM Grant Agreement No. 779391

“The FutureTPM project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 779391.”

If you need further information, please contact the coordinator:

TECHNIKON Forschungs- und Planungsgesellschaft mbH
Burgplatz 3a, 9500 Villach, AUSTRIA
Tel: +43 4242 233 55 Fax: +43 4242 233 55 77
E-Mail: coordination@futuretpm.eu