P3.3-764

Methodology For Monitoring the Correctness Of the Transmission Of Data Received From the Devices Of the CTBTO On-site Inspectors

A. Mukhortova, V. Afonin

National Research Nuclear University MEPhI (Moscow Engineering Physics Institute)

MEPhI
National Research
Nuclear University

INTRODUCTION AND MAIN RESULTS

This presentation outlines essential security requirements for OSI data transmission — integrity, authenticity, and non-repudiation — and compares HMAC and digital signatures as solutions. We provide practical implementation guidelines tailored to CTBT verification needs.

SnT 2025
8 SEPTEMBER ONLINE DAY
9 TO 12 SEPTEMBER AT HOFBURG PALACE, VIENNA & ONLINE
CTBT: SCIENCE AND TECHNOLOGY CONFERENCE

Methodology For Monitoring the Correctness Of the Transmission Of Data Received From the Devices Of the CTBTO On-site Inspectors

A. Mukhortova, V. Afonin

P3.3-764

Introduction

During on-site inspections, inspectors collect critical sensor data from monitored areas with their tablets. This data must be securely transmitted to the server while ensuring:

- **Integrity** — the data has not been altered in transit.
- **Authentication** — the data originates from a trusted inspector.
- **Non-Repudiation** (if required) — the inspector cannot later deny submitting the data.

To achieve this, two approaches are commonly used:

HMACs and **Digital Signatures**

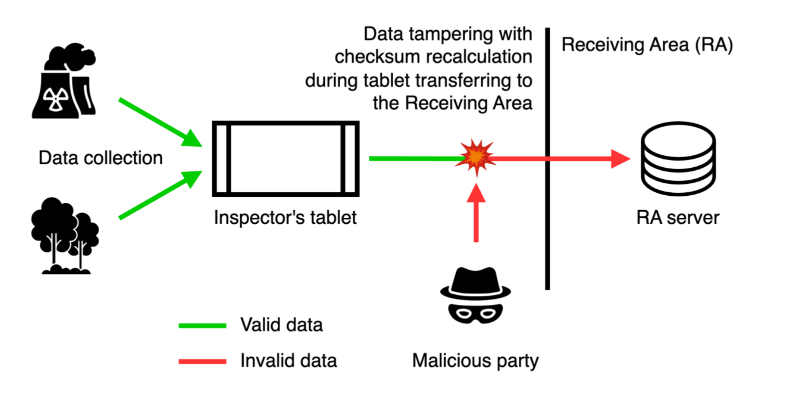

Figure 1. Concrete scenario that leads to invalid data being transferred to the server in the Receiving Area.

This e-poster explores the possibilities of using HMACs and digital signatures for preserving data integrity, authentication and (optionally) non-repudiation.

Why does it matter for the CTBTO inspections?

- Prevents tampering with sensitive nuclear test data.
- Ensures that only authorized inspectors submit verified readings.

Which method is the best for OSI? Let's compare!

Methods/Data

What are the ways to monitor the correctness of the transmission of data?

- **HMAC**. A *symmetric* mechanism used to verify integrity and authenticity of a message using the same shared secret key for both generation and verification.

$$HMAC_K(M) = H((K \oplus opad)||H((K \oplus ipad)||M))$$

where H — hash function, M — message to be authenticated, K — secret key, $opad$, $ipad$ — special paddings.

- **Digital Signature**. An *asymmetric* mechanism used to verify the integrity, authenticity, and non-repudiation of a message using a private key for signing and a public key for verification.

If it is required to limit the number of people who can verify the signature, one can use the **Designated Verifier Signature (DVS)**, which allows one to give the right to verify the signature to a specific verifier.

Multi-designated Verifiers Signature (MDVS) is used to allow a group of users to verify the signature. This can be used to allow the CTBTO servers and the inspected party to verify inspection data.

Universal Designated Verifier Signature (UDVS) is used to convert DVS to common signature when it's needed to reveal the signature to general public. On-site inspectors may use this signature to protect themselves from being blackmailed by the inspected party.

MEPhI
National Research Nuclear University

Methodology For Monitoring the Correctness Of the Transmission Of Data Received From the Devices Of the CTBTO On-site Inspectors

A. Mukhortova, V. Afonin

P3.3-764

Results

We have conducted the benchmarks comparing the two approaches: an HMAC and a Digital Signature. We chose the **ECDSA signature algorithm** as one of the widely used production algorithms and an HMAC instantiated with the SHA-256 hash function. Our benchmark code is open source and available under the permissive license.

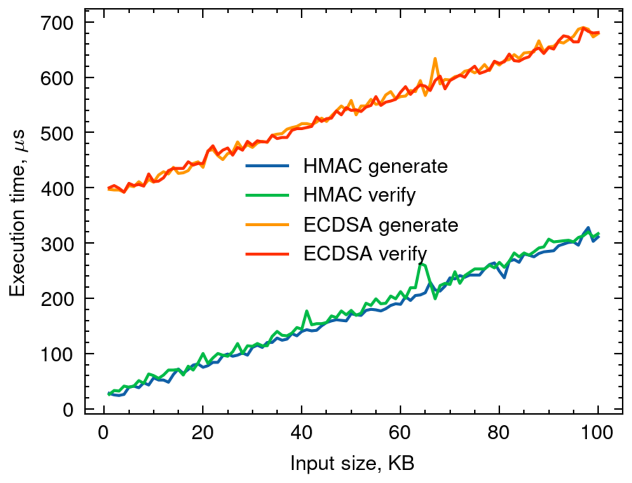

Figure 2. Comparison of HMAC and ECDSA execution times. Both algorithms are instantiated with the SHA-256 hash function. The benchmarks were conducted on the AMD Ryzen 5 5600G with Radeon Graphics 3.90 GHz with 32 GB RAM and Windows 10 22H2 operating system.

Criterion	**HMAC**	**Digital Signature**
Type of key	Symmetric (shared key)	Asymmetric (public + private key)
Non-Repudiation	No	Yes
Additional participant	Requires shared key pair	Yes, easy
Data Aggregation	No Data Aggregation	Aggregated signature schemes exist
Post-quantum resistance	Yes	Only with specific post-quantum signature schemes
Performance	Faster	Slower
PKI requirement	No PKI required	PKI required

Table 1. HMAC and Digital Signature comparison.

The table above compares two basic methods of verifying message integrity: HMAC and digital signature. As we can see, each method has both significant drawbacks and advantages. Therefore, there is no definitive answer as to which method should be used by the OSI personnel. However, HMAC should be used when resources and time are limited, while digital signatures should be used when more security properties are required. Thus, it is possible to use either method or a combination of both during on-site inspections.

Conclusion

For optimal security, use HMAC for high-volume operational data with strict key rotation, while reserving digital signatures for critical evidence with robust PKI. This tiered approach ensures uncompromising integrity while balancing performance needs across all inspection phases.

Additionally, Designated Verifier Signature (DVS), a relatively new integrity-checking method has been introduced that enables signature verification by a restricted set of verifiers. This is critical for handling sensitive data and mitigating third-party blackmail risks against the signee.

To further support our evaluation of these approaches, we have developed an open-source benchmark that provides a comprehensive performance comparison between HMAC and digital signatures. Our code is available under a permissive license, allowing contributors to freely use, modify, and extend the benchmark to capture other use cases.

MEPhI
National Research
Nuclear University