WHITE PAPER

# Secure updates of Windows-based applications

December 2025

AXIS COMMUNICATIONS

# Summary

At Axis we use TUF (The Update Framework) to provide secure software updates for our Windows-based applications. TUF ensures the security and trustworthiness of software updates by verifying that they are signed by a trusted source. TUF also helps us comply with regulatory and industry standards for software distribution, and it is flexible enough that we can adapt it to our specific workflows and infrastructure needs.

The implementation design of TUF anticipates that repositories will likely be compromised at some point. Therefore, TUF-enabled systems prioritize containment and recovery. By separating signing duties and requiring multiple signatures, TUF limits the damage caused by a single compromised key or entity. The framework provides a set of security protocols, including content signing, verification, trust management, and freshness, to ensure the security of software updates. As a consequence, it protects you as an end user as well.

# Table of Contents

# 1 Introduction

At Axis we use The Update Framework (TUF) to provide secure software updates for some of our Windows-based management software (AXIS Camera Station Pro and AXIS Audio Manager Pro). This framework ensures the integrity and authenticity of software updates, preventing supply chain attacks and tampering.

This white paper describes the software update service and how it is implemented at Axis.

# 2 Background

Software updates are essential for maintaining the security of applications. A patch can add functionalities and address flaws in existing code. However, if not implemented properly, updates can be vulnerable to attacks and tampering and compromise the entire system. Traditional update methods often rely on trusting the update channel and intermediaries, which can be a weak link in the security chain.

You regularly need to update management software such as AXIS Camera Station Pro or AXIS Audio Manager Pro. You might not always need the latest version, but when you update, the download and installation process must be secure. The automatic update service through Axis ensures a safe and smooth procedure that follows the standardized, security-audited TUF protocol.

# 3 Overview of TUF

The Update Framework (TUF) is a widely used software framework designed to protect mechanisms that automatically identify and download updates to software. TUF employs a system of roles and encryption keys to maintain security, even when some keys or servers are compromised. This way, TUF effectively protects software repositories, which are an attractive target for cyber-attacks. As a consequence, end users are protected as well.

TUF takes a proactive stance against potential security threats by assuming that software repositories will inevitably be compromised. In response, TUF-enabled systems concentrate on mitigating the consequences of a breach, rather than solely relying on prevention measures. By decentralizing authentication tasks and introducing multi-party verification protocols, TUF reduces the attack surface and minimizes the impact of a breach.

The main security protocols provided by TUF are:

- **Content signing.** Developers sign software updates using cryptographic keys that ensure authenticity.
- **Verification.** Users who download the software update can verify the signature, ensuring that the content has not been tampered with during transit.
- **Trust management.** TUF enables the management of trust, allowing for the revocation and rotation of signing keys if they are compromised.
- **Freshness.** TUF ensures that updates are delivered in a timely manner, preventing replay attacks.
- **Delegation.** Administrators can grant developers the right to make releases for specific applications or tracks.

TUF (*https://theupdateframework.io/*)

Notary (*https://github.com/notaryproject/notary*)

# 4 Implementation at Axis

Axis uses the open-source project Notary to implement TUF. Notary can certify the validity of the sources of software updates. It also secures operations for Microsoft Azure where the update files are stored.

The Notary backend has clients running on the sites, in this case on Axis network and on your computer.

## 4.1 Why Axis adopts TUF

We've chosen to work with Notary based on several important aspects, the main one being improved security. Notary is a reliable and mature implementation of TUF that is widely used in the industry and has undergone multiple public security audits.

Employing the framework also helps us meet regulatory and industry standards for software integrity and distribution. Furthermore, the flexibility of Notary being an open-source project allows us to adapt it to our specific workflows and infrastructure needs. It's also scalable, TUF being designed to handle large-scale software and container distribution systems.

## 4.2 System of roles and encryption keys

As specified by TUF and implemented by Notary, we secure the update process through a system of roles and encryption keys.

- **Key management.** Private keys are password-protected and encrypted. Compromised keys can be revoked and rotated to prevent further attacks.
- **Root of trust.** The root key is stored in a secure location, only accessible by authorized personnel.
- **Multiple metadata files.** Notary uses multiple metadata files, including root, timestamp, snapshot, and target files. The timestamp and snapshot files specifically prevent replay attacks and ensure freshness.
- **Delegation files.** Delegation files are used to grant developers the right to make releases for specific applications or tracks.

## 4.3 About the Notary backend

**Metadata files.** The Notary backend holds at least four metadata files (root, timestamp, snapshot, and target) and several delegation files. There is one delegation file for each application you want to release (for example AXIS Camera Station Pro).

**Key management.** The root (root of trust) is signed with the root key, which is stored in a digital vault at Azure and is only accessible by a very limited number of administrators. The root key is used to create all other keys. Your update agent (UA, the software component responsible for managing and applying updates in your computer) can check the root file to see which keys the metadata files were signed with.

**Roles.** Root, target, snapshot, and timestamp are different roles in the TUF framework. In TUF, you always minimize individual key risks and role risks. If keys become compromised (and the attacker also has the password and decrypted the keys), there will be only limited negative consequences. If someone attacks the Notary backend, they will only get access to timestamp and snapshot, not other keys that would be needed to create illegitimate releases. As long as the root key is not compromised, there's no worry.

To create illegitimate releases, a person would need delegation and target keys. Delegation keys are required to make releases for a particular application, but they are distributed to only a few individuals at Axis. The target key can be used to create new delegations, but it is kept in a secure place only accessible to the update service administrator at Axis. Should the Notary backend be compromised, updates can no longer be distributed correctly. No client can be deceived into installing a compromised application without access to any of these encrypted keys.

**File functionality.** All files have a short lifespan and are regenerated frequently:

Target file

- Lists all registered public keys and their permissions.

Snapshot file

- Contains hashes for all the other files. The snapshot role is responsible for keeping track of the overall state of the files in the repository.
- Is signed with its own key.

Timestamp file

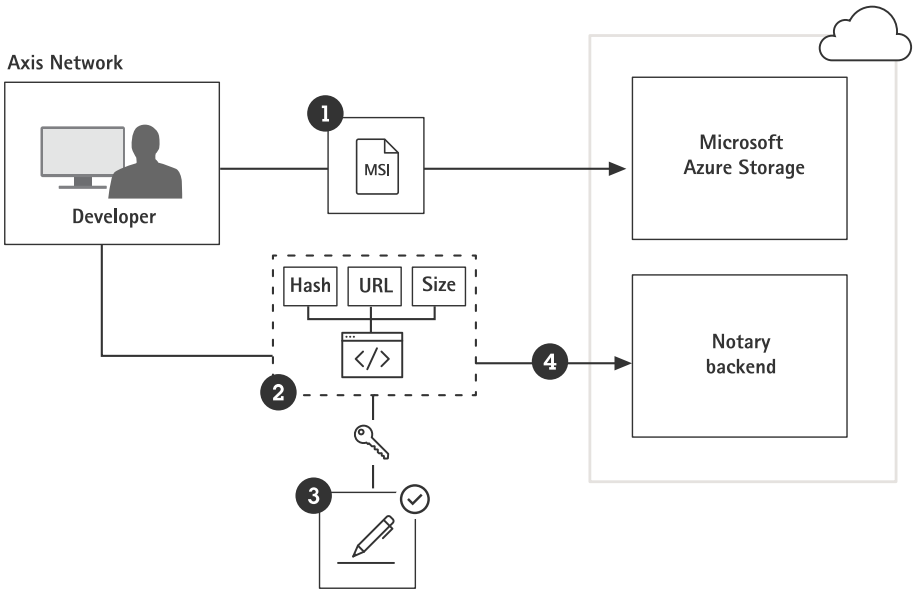
- Contains a hash of the snapshot file.
- Protects against replay attacks. When the UA polls, it downloads the timestamp file. It will download the snapshot file only if the timestamp shows that the snapshot file has changed.

# 5 Workflow of Axis software updates

Processes are in place to verify the legitimacy of Axis software updates, both when Axis uploads the update to the cloud and when you download the update to your computer. These processes comply with the TUF framework.

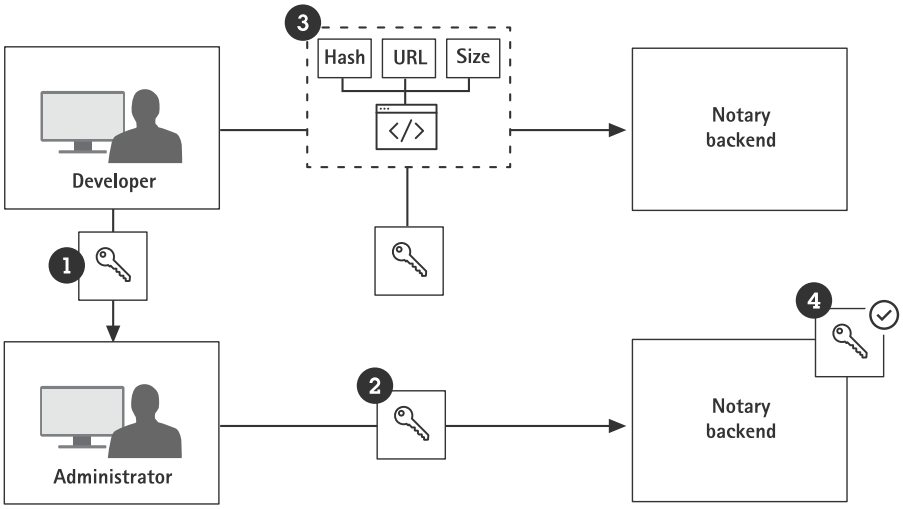
## 5.1 Secure uploads from Axis network

A developer uploads a software update to the cloud and a signed metadata file to the Notary backend. Axis administrators are also involved in the process by sharing the developer's info and public key with the Notary backend. This way, the Notary backend can verify that the software update is legitimate.




*A developer uploads a software update to the cloud and a signed metadata file to the Notary backend.*

1. ***Update preparation and upload.*** *The developer prepares a software update (for example an msi file) and uploads it to Microsoft Azure Storage.*
2. ***Metadata creation.*** *The developer creates a metadata file for the update, including hash, url, and size for the msi file.*
3. ***Metadata signing.*** *The developer signs the metadata file using an encrypted private key and password.*
4. ***Metadata upload.*** *The developer uploads the signed metadata file to the Notary backend. Through a series of steps the Notary backend can verify that the metadata was correctly signed by the developer.*




*Details of the metadata upload*

1 *The developer sends the public key to the administrators.*
2 *The administrators upload the public key to Notary backend. They also upload information about which software the developer is authorized to publish updates to.*
3 *The developer uploads the metadata to Notary backend with the help of the keypair of a public and private key.*
4 *Notary backend verifies, using the developer's public key, that the metadata was correctly signed by the developer.*

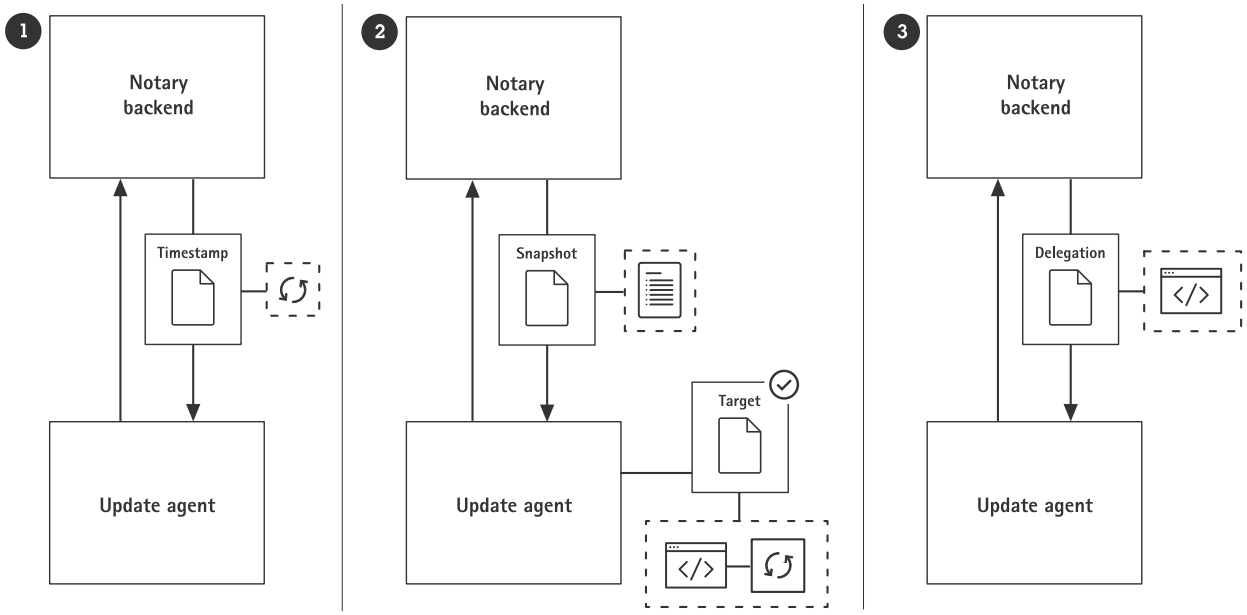
## 5.2 Secure downloads to your computer

A UA (update agent) downloads new software updates and installs them securely by communicating with the Notary backend. The UA doesn't download software directly from the Notary backend but instead uses the Notary client on your computer.

Both the update agent and the Notary client are included with your purchase of Axis management software. They're installed on your computer and the update agent is connected to your copy of AXIS Camera Station Pro or AXIS Audio Manager Pro.

### 5.2.1 Polling for updates

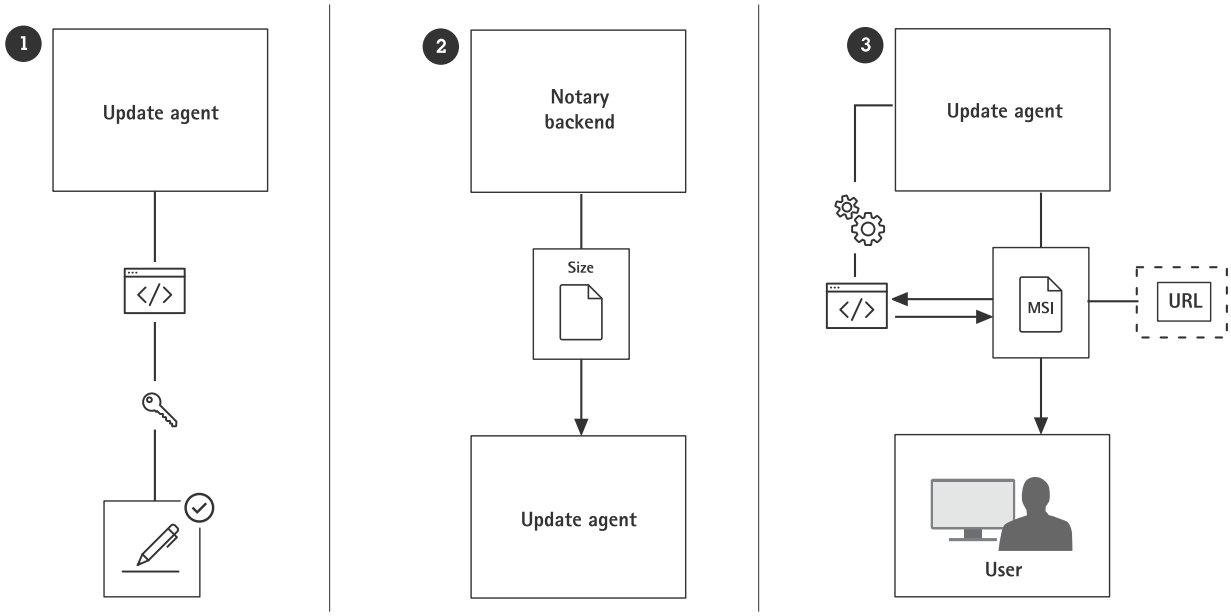
The UA (update agent) on your computer polls the Notary backend at regular intervals for new updates.




*The polling process*

1 ***Request and timestamp verification.*** *The UA sends a request to Notary backend to check for new updates. The backend responds with the timestamp file, which contains the latest update information.*
2 ***Snapshot file verification and target file verification.*** *If the timestamp file indicates a new update, the UA requests the snapshot file, which contains a list of all the files in the repository. The UA verifies the target file, which holds the metadata for the specific update.*
3 ***Delegation file verification.*** *If the target file indicates a new update, the UA requests the delegation file, which holds the metadata for the specific application or track.*

### 5.2.2 Verifying and downloading the update




*Verification process for the download.*

1 *The UA verifies the signature of the metadata and ensures it was signed by a trusted key.*
2 *The UA retrieves the size file to know how large the update file should be.*
3 *The UA uses the URL to download the update file (for example an msi file) to your computer, checks the hash, and compares the metadata file with the update file.*

The .msi file extension is a Windows Installer format that uses Microsoft's Windows Installer service to configure installer packages, such as Windows applications or update packages.

# About Axis Communications

Axis enables a smarter and safer world by improving security, safety, operational efficiency, and business intelligence. As a network technology company and industry leader, Axis offers video surveillance, access control, intercoms, and audio solutions. These are enhanced by intelligent analytics applications and supported by high-quality training.

Axis has around 5,000 dedicated employees in over 50 countries and collaborates with technology and system integration partners worldwide to deliver customer solutions. Axis was founded in 1984, and the headquarters are in Lund, Sweden.