Attestation Statements & Privacy Impacts

Supported Attestation Statements in PoM

Android SafetyNet

- Attestation Statement Format Identifier
- :android-safetynet
- Supported Attestation Types
- : Basic
- Syntax
- : The syntax of an Android Attestation statement includes fields likefmt
- (format) set to "android-safetynet" andattStmt
- (attestation statement) which contains the SafetyNet statement format. This format has two fields:ver
- , which is the version number of Google Play Services responsible for providing the SafetyNet API, andresponse
- , which is the UTF-8 encoded result of thegetJwsResult()
- call of the SafetyNet API.
- Privacy Impact
-

Imagine a manufacturer named "TechGiant" produces a series of smartphones. Each series has a unique identifier, let's say "TG2023Pro". Now, within this series, there are thousands of individual devices, each with its unique device ID.

When an application on an Android device from this series uses the SafetyNet Attestation, the attestation result might include a field, let's call it "DeviceBatchInfo". This field doesn't reveal the exact unique device ID, which would directly identify the individual device. Instead, it provides the series identifier, "TG2023Pro".

1. No Direct Identification
2. : The attestation doesn't directly reveal which exact device from the "TechGiant" manufacturer made the request. So, an individual's specific device isn't directly exposed.
3. Batch Information Exposure
4. : However, it does reveal that the device belongs to the "TG2023Pro" series. This can have implications in scenarios where certain batches or series of devices have known vulnerabilities, characteristics, or are associated with certain demographics or regions.
5. Potential for Profiling
6. : Over time, if various apps or services collect such batch information, it might be possible to build a profile of the kind of devices a user owns or prefers. For instance, if a user consistently shows up with attestations from high-end device batches, services might infer that the user prefers premium devices.
7. Aggregate Data Analysis
8. : On a broader scale, if a service collects attestation results from many users, they might be able to analyze trends, like which device batches are more popular, which ones have more security-conscious users, etc.
9.

In essence, while the Android SafetyNet Attestation doesn't directly expose the exact device, the batch or series information can still have privacy implications, especially when combined with other data or when analyzed in aggregate.

TPM

- Attestation Statement Format Identifier
- :tpm
- Supported Attestation Types
- : AttCA
- Syntax
- : The TPM attestation statement is conveyed by populating thefmt
- field of theattStmt
- structure with the string "tpm". TheattStmt
- structure also contains thever
- field, which represents the version of the TPM specification to which the TPM adheres. Additionally, thealg
- field indicates the algorithm used by the TPM to compute the signature, and thex5c
- field provides the certificate chain that proves the attestation key resides in a genuine TPM.
- Privacy Impact
-

The use of TPM attestation can have privacy implications. When TPM attestation is used, it can potentially allow relying parties to track users based on the unique TPM attestation certificates. This is because each TPM chip has a unique Endorsement Key (EK), and the attestation certificate is tied to this unique key. If the same TPM is used across multiple services, it can be used to correlate user activities across these services.

Imagine a user, Alice, who uses her device's TPM for authentication on two different online platforms - Platform A and

Platform B. Both platforms receive the TPM attestation certificate during the authentication process. If both platforms were to share data or have a common third-party tracker, they could potentially determine that Alice is the same user on both platforms based on the unique TPM attestation certificate. This could lead to a breach of Alice's privacy as her activities on both platforms can be correlated.

It's essential to be aware of these privacy implications when implementing or using TPM attestation and to take necessary precautions to protect user privacy.

Generic Packed

- Attestation Statement Format Identifier
- :packed
- Supported Attestation Types
- : Basic, Self, AttCA
- Syntax
- :
-
    - fmt
-
    - : A string that indicates the attestation statement format. For the Generic Packed Attestation, this value is set to "packed".
-
    - attStmt
-
    - : This is the attestation statement. It contains the following fields:
-
    -
        - alg
-
    -
        - : A number that represents the algorithm identifier used for the attestation signature.
-
    -
        - sig
-
    -
        - : A byte array containing the attestation signature.
-
    -
        - x5c
-
    -
        - : An optional array of byte arrays. This field is present when the attestation type is either Basic or AttCA. It contains the attestation certificate and its possible chain, each encoded in X.509 format.
-
    -
        - ecdaaKeyId
-
    -
        - : An optional byte array. This field is present when using ECDAA attestation to identify the ECDAA-Issuer public key. (Note: This is relevant for ECDAA attestation, which is not one of the primary three types we discussed but is another possible attestation method.)
-
    -
        - cosePublicKey
-
    -
        - : An optional byte array. This field is present when using self attestation, and it contains the COSE-encoded public key.

-
    -
- It's important to note that the presence of certain fields, such asx5c
- andcosePublicKey
- , depends on the type of attestation being used (Basic, Self, or AttCA). The exact structure and content of the attestation statement will vary based on the attestation type and the specific details of the authenticator and the attestation process.
- Privacy Impacts

- Basic Attestation
- Privacy Impact:
- This type of attestation provides a certificate that can be traced back to a specific batch or model of authenticators. If the certificate is unique to each device or has identifiable information, it can be used to track users across different services.
- Example:
- If Alice uses her device to register with multiple services, and each service collects and stores the attestation certificate, these services could potentially determine that Alice is using the same device across all platforms, thereby compromising her privacy.

- Self Attestation
- Privacy Impact:
- In this mode, the authenticator uses a certificate that might be shared among multiple devices of the same model or batch. While this does not directly reveal the exact device, it can still provide insights into the device's make or model. However, since many devices might share the same self attestation certificate, it offers a higher degree of privacy compared to basic attestation.
- Example:
- If Bob and Charlie both have the same device model and use it on a platform, the platform cannot distinguish between Bob's and Charlie's devices based solely on the self attestation certificate.

- Attestation CA (AttCA)
- Privacy Impact:
- The AttCA mode provides a balance between user privacy and attestation assurance. The attestation key is certified by an Attestation CA, but the certificate does not contain specific details about the individual device. While it offers more privacy than basic attestation, there's still a potential risk if the Attestation CA logs requests and shares them, as this could be used to track which services a user is registering with.
- Example:
- If Alice registers her device with Service X and Service Y, and both services verify the attestation with the same Attestation CA, the CA could potentially know that Alice's device was used to register with both services, even if the services themselves cannot directly identify Alice's device.

- *
-

In summary, while each attestation type in the Generic Packed Attestation offers a level of assurance about the authenticity of the authenticator, they have varying degrees of privacy impact. It's essential to choose the appropriate attestation type based on the specific use case and the desired balance between assurance and user privacy.

In PoM Demo, we choose to use AttCA type for Yubikey Packed attestation, whose privacy impact follows the AttCA cases

in Generic Packed Attestation.

References

- Android SafetyNet Attestation Statement Format
- TPM Attestation Statement format
- Packed Attestation Statement Format
-

Previous WebAuthn Attestation Types Next Software Build Attestation Last updated7 hours ago On this page *Supported Attestation Statements in PoM * Android SafetyNet * TPM * Generic Packed * References

Was this helpful?