Chapter 1

Look Inside

Trusted GAT Results

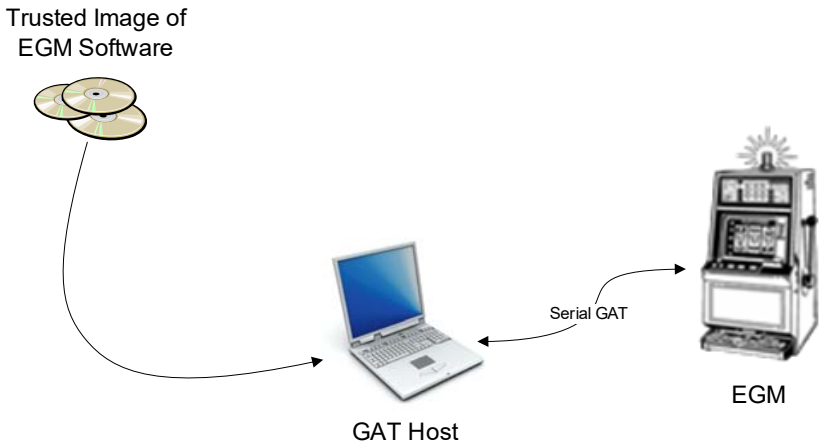
Overview

1.1 Introduction

This document contains the specifications for a standard file format that can be used to convey a list of trusted GAT (Game Authentication Terminal) results to a GAT host. The GAT results correspond to specific components that are exposed by an EGM, or other type of end-point, to a GAT host. The schema for the file format accompanies this document.

A problem that both regulators and systems manufacturers face today is how to trust GAT results returned from an EGM, or other end-point. Without an alternative mechanism, results returned over GAT can only be validated by comparing the value returned by the end-point to a value calculated by the GAT host against a trusted version of the software being challenged. This forces the software performing GAT, which may be run on a download system or regulator's laptop, to understand how all manufacturer software is built so that it can calculate a trusted hash value for the software. This can be difficult due to technology diversity in the industry and changes to software packaging over time. One example is illustrated in the following diagram:

Figure 1.1 GAT Example



This specification helps to resolve this issue by allowing the software manufacturer, regulator, or test lab to publish a file containing a set of trusted GAT values for the regulated software in a secure manner. This allows a GAT host to simply compare the value returned by the end-point being challenged to the values stored in the trusted file. If the value returned by the device being challenged is not in the trusted file, the GAT host can consider the GAT result invalid and take appropriate action. On the other hand, if the result returned matches a value in the trusted file, the GAT host can inform the operator running the system that the GAT comparison was successful.

1.1.1 Product

This specification relies upon the concept of components and products. The product concept was first introduced in the GSA Manifest Package File Format specification. It describes a typical "product" that an operator purchases from a manufacturer. Typically, products are downloaded using G2S or S2S and installed on an EGM or other end-point. Examples of products include game content, such as Win Like a Wild Man, peripheral firmware updates, and even operating system updates. See the GSA Package Manifest File Format for the requirements for constructing product identifiers.

1.1.2 Components

Products contain "components" which can be directly challenged using GAT. A component can be firmware for a physical device or a software module on an end-point – for example, firmware for a ticket printer or bill validator; or, software such as server-side executables, DLLs, or downloadable content for an EGM. See the G2S Message Protocol and the S2S Message Protocol for the requirements for constructing component identifiers.

1.1.3 Security

Trusted GAT files MUST be digitally signed by their author so that recipients of the files can verify that they have not been manipulated. Trusted GAT files MUST be signed as follows:

- Cryptographic Message Syntax (CMS) MUST be used - RFC 5652
- A SignedData ContentType MUST be used, with the Trusted GAT XML as the encapsulated content
- All certificates required to re-create the certificate chain from the signer to the trusted root certificate MUST be included in the CMS message
- At a minimum, SHA-1 with RSA 2048 bit keys MUST be used.
    - An implementation MAY support SHA-256 or SHA-512 with RSA 2048 bit keys or greater. Please see RFC 5754 for more information about use of these algorithms with CMS.
    - An implementation MAY support SHA-256 or SHA-512 with ECDSA. Please see RFC-5753 for more information about use of these algorithms with CMS.

1.1.4 Trusted GAT File Extension

Trusted GAT files MUST be written to storage media with a file extension set to ".gsaTrusted".

1.1.5 Trusted GAT Import

Trusted GAT files are expected to be distributed with the software packages that they verify using the approach specified in Section 1.8 Product/Package Import of the GSA Package Manifest File Format specification.

When distributed with a GSA package manifest file, the trusted GAT file MUST be located in the same folder as the GSA package manifest file.

It is also possible for trusted GAT files to be distributed separately from the software packages that they verify, especially if they are created by a regulator or testing laboratory.

When needed to meet regulatory or other requirements, trusted GAT files may be accessible over a network from a trusted source.