

## Benefits

- Full GBA Implementation for mobile TV
- High Scalability and Redundancy
- Flexible Deployment
- High-security from a security specialist
- Bootstrapping keys are stored in encrypted form in the database
- A SafeNet HSM can be added on demand
- All critical communications links are encrypted, e.g. TLS on the Zn' interface.
- Logging and Monitoring
- Performance Monitoring
- BSF was tested at the bmco forum test camp in Berlin
- Ongoing IOT testing

# DRM Fusion BSF & GBA Components

Mobile TV holds tremendous potential to generate revenue for mobile operators, provided solutions are secure and support flexible business models. SafeNet's DRM Fusion Toolkit4TV is the leading software-based security solution for mobile TV that addresses these problems. The solution is the first-of-its-kind to incorporate MBMS Security and the OMA BCAST Smartcard Profile, emerging open standards for mobile TV protection.

Mobile operators also want to ensure mobile TV solutions maintain operator user ownership, and minimize deployment costs. MBMS Security and OMA BCAST Smartcard Profile provide these capabilities through use of the SIM for security, and using the Generic Bootstrapping Architecture (GBA) to access an operator's existing voice authentication infrastructure.

GBA mutually authenticates the SIM and the operator network during service access initiation. The derived keys are then used to protect SEKs so that they can only be accessed by a particular device.

In response to growing concerns that GBA costs could potentially hinder mobile TV deployments, SafeNet has brought a cost-effective bundle of GBA components to market, focused specifically on mobile TV enablement. These components include a Bootstrapping Server Function (BSF), an HSS/HLR proxy, and a Zn proxy.

## A full GBA Implementation for Mobile TV

SafeNet provides a full GBA implementation which can be used with Universal Subscriber Identity Modules (USIMs) or IP Multimedia Services Identity Modules (ISIMs).

## Security

All confidential information, such as bootstrapping keys, is encrypted and stored in the component's databases. All critical communications links are encrypted, e.g. TLS on the Zn' interface.

A SafeNet Hardware Security Module (HSM) can be deployed for key storage or to execute cryptography functions if enhanced security is desired.

## Scalability and Redundancy

SafeNet GBA components are fully scalable and can be deployed in a redundant configuration.

## Logging and Monitoring

SafeNet GBA components' event management system is used to direct application events to event propagators, e.g. a log propagator which writes the event to a log file. Event generators within the application create and fire events which are then directed by the event manager to propagators registered for that event.

The events received by each propagator are configurable. Among the default propagators (custom propagators can also be added) is an SNMP event propagator which sends SNMP traps corresponding to the events it receives.

This feature enables operators to monitor activities including but not limited to:

- Number of transactions in the last reporting period for Ub interface
- Number of transactions in the peak second of the last reporting period for Ub interface
- Number of transactions in last reporting period for Zn interface
- Number of transactions in the peak second of the last reporting period for Zn interface
- Number of stored security associations

## Performance Monitoring

Configurable performance counters can be generated—reporting the number of Zn requests in the a specific period of time and number of transactions in the peak second of the last reporting period for Ub.

## Flexible Deployment

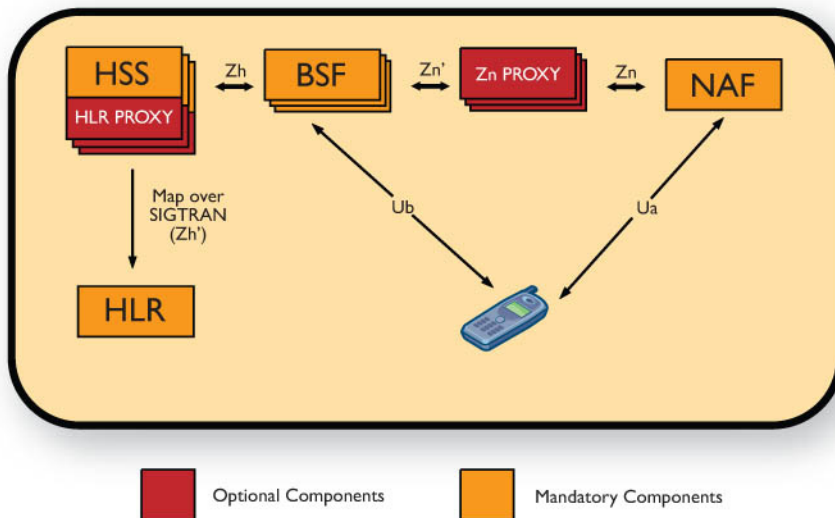
The BSF component can interact with an existing HLR or act as a stand-alone HSS. Since the standardized Zn interface is supported, the entire GBA implementation can be replaced if necessary with no effect on the other components.

## Distributed Deployment

SafeNet BSF and GBA components consist of logically separate components; the HSS/HLR proxy, the BSF, and the Zn proxy therefore allowing for flexible deployment since the modules are distributable. Deployment of these components on physically distinct servers is also supported. However, it is recommended to co-locate the HSS/HLR proxy and the BSF.

## About SafeNet DRM Solutions

SafeNet is a global leader in information security. Founded more than 20 years ago, the company provides complete security utilizing its encryption technologies to protect communications, intellectual property and digital identities, and offers a full spectrum of products including hardware, software, services and chips. SafeNet is firmly committed to the development and delivery of flexible, future-proof, standards-based DRM solutions. Successful online content delivery depends upon providing a compelling user experience, and SafeNet is addressing this issue through innovation in ease of use and interoperability testing for DRM. The company is an active member of several industry associations including the BMCoforum, the Mobile Entertainment Forum, and the Open Mobile Alliance. UBS, Nokia, Fujitsu, Hitachi, Bank of America, Adobe, Cisco Systems, Microsoft, Samsung, Texas Instruments, the U.S. Departments of Defense and Homeland Security, the U.S. Internal Revenue Service and scores of other customers entrust their security needs to SafeNet. In 2007, SafeNet was taken private by Vector Capital.



### Components:

#### BSF:

Mutual authentication using the AKA protocol - The BSF and UE interact over interface Ub in order to mutually authenticate using the AKA protocol.

#### Supports Ub, Zn and Zh interfaces

The BSF supports interface Zn, which allows the Network Application Function (NAF) to fetch the key material previously agreed during a HTTP Digest AKA protocol run over reference point Ub. The BSF also supports interface Zh to the HSS/HLR proxy. The BSF requires a database to store bootstrapping session data.

#### Zn Proxy:

Validates to the BSF that the NAF is authorized -- The Zn-Proxy functions as a proxy between the NAF and the BSF. The proxy validates that the NAF is authorized to participate in GBA and asserts to the BSF the NAF's DNS name.

#### Supports Zn and Zn' (TLS) interfaces

The Zn' interface between the Zn proxy and the BSF can be secured using TLS.

#### HSS/HLR Proxy:

Retrieves authentication vectors from the HLR, over MAP:SIGTRAN interface -- The HSS is a fully functional GBA HSS which manages GUSS, secret keys K, etc. However, this component can also act as a proxy to an existing HLR by retrieving authentication information from the HLR over SIGTRAN.

#### For information about DRM products:

North America — SafeNet Irvine	949.450.7300
Europe — SafeNet Amsterdam	+31 20 3303372
Asia Pacific — SafeNet Hong Kong	852.3157.7111
Email: <a href="mailto:drmproductsinfo@safenet-inc.com">drmproductsinfo@safenet-inc.com</a>	

**Corporate Headquarters:** 4690 Millennium Drive, Belcamp, Maryland 21017 USA  
Tel.: +1 410 931 7500 or 800 533 3958, Fax: +1 410 931 7524, Email: [info@safenet-inc.com](mailto:info@safenet-inc.com)

**EMEA Headquarters:** Tel.: + 44 (0) 1276 608 000, Email: [info.emea@safenet-inc.com](mailto:info.emea@safenet-inc.com)

**APAC Headquarters:** Tel: +852 3157 7111, Email: [info.apac@safenet-inc.com](mailto:info.apac@safenet-inc.com)

For all office locations and contact information, please visit [www.safenet-inc.com/company/contact.asp](http://www.safenet-inc.com/company/contact.asp)

[www.safenet-inc.com](http://www.safenet-inc.com)