3GPP TSG SA WG3 Security — S3#20 S3-010600
27 - 30 November, 2001
Sophia Antipolis, France

GENERAL PURPOSE AUTHENTICATOR VIA MOBILE PHONE

Doc No:		Date Issued:	29/10/01	Copy No:
Version:	**0.4**	Version Status:	DRAFT	
Category:	Reference	Author:	Stuart Ward	

Comments:

General Purpose Authenticator via Mobile Phone

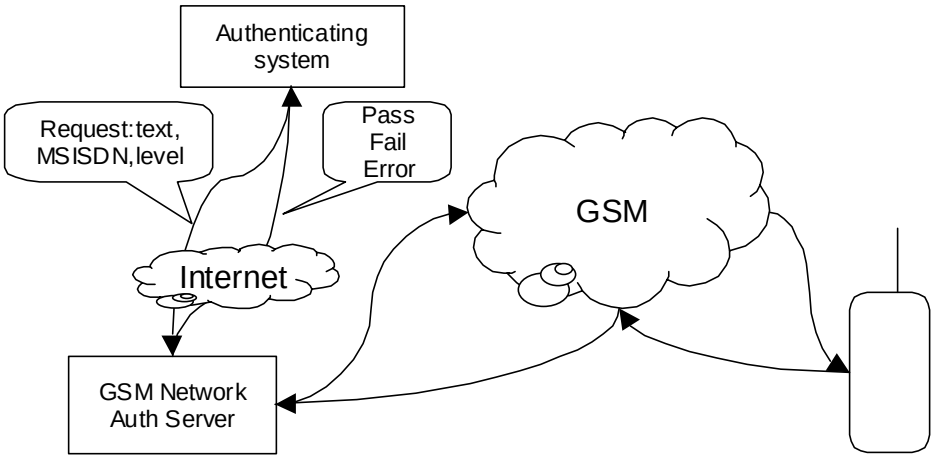
1. Scope

In this paper I describe a service that could provide an authentication step by using the physical possession of a GSM phone to accept a transaction or authorise a system access.

There are many places that require authentication. From access control of systems to authenticating transactions for payment where the parties are not physically present and the use of physical verification, i.e. signature is not possible or sufficient.

This proposal describes a relatively simple service that could be the first step towards using a mobile handset for a full m-Commerce solution. This would help to educate users in the capabilities of their mobile and help to foster a perception of the mobile as a "secure" device.

2. Proposal



A system requiring authentication would send an authentication request to the GSM operator's Authentication server. This request would have a previously registered mobile number associated with the account (MSISDN) from which the authorisation is required. The message is sent over the Internet, or other network, using a secure and authenticated connection to the GSM operators' server for processing these requests. The Auth Server then performs a set of checks on the GSM network with the MSISDN according to the level of authentication required and then replies with a success or failure of the authentication.

I have listed here some ideas for methods of authentication that would be possible. Some levels of authentication may not be possible depending on the capabilities of the network, mobile handset or SIM card involved.

2.1 Valid MSISDN account

This request would only check that the MSISDN was a valid account on the operators' network. This step could be done as the first step in registering a mobile with an account.

2.2 MSISDN is attached to the network

This request will verify that the current IMSI associated with this MSISDN is either attached to the home network or attached to a roaming network. The Auth Server will establish this by requesting records from the HLR/VLR for current

connection status. It could possibly return the time of the last location update or call activity to indicate how recent this information is. This level may be used in the next level of registration, but is probably not going to be used much. It does have the advantage that responses to this request only require server requests so the time to perform this request would be quick.

2.3 Successfully send an SMS to the mobile

This level of request would attempt to send the "text" in the request as a SMS message to the mobile. If the mobile accepts the SMS message immediately then this would be a success. If not the authentication would fail. This would require the setting of a timeout value after which the request will be deemed to have failed. If the message is not successfully sent then this message is NOT stored for later transmission like a normal SMSC but discarded, and the result returned to the requestor. The case of the mobile failing to be able to receive the message because its internal message store is full would need to be defined.

2.4 Successfully send a USSD message to the mobile

Exactly in the same manner as the SMS message, a message would be sent as a USSD structured string to the mobile. The mobile would then respond back with a accept or error message back to the Auth Server. This would probably require a SIM Tool Kit (STK) application to process this request and respond. This approach would remove failures because the message store was full on the mobile.

2.5 Require user acceptance.

At this level the USSD message to the mobile will present the text and ask the user to accept or reject the message. This response is then returned to the Auth Server and then back to the requestor. A no user response time out will need to be defined. I imagine that this would be of the order of 10 to 20 seconds. The USSD protocol allows for this without any further facilities on the phone. A more sophisticated version could trigger a STK application to encrypt the response.

2.6 Require user PIN acceptance

At this level the USSD message will trigger a STK application that will require acceptance and will also ask for the entry of a PIN number to verify the user. The PIN number could either be checked with a secure location on the SIM card or it could be encrypted and sent back to the server for checking. Care would need to be taken on how to handle errors in entering the PIN number should the system retry a number of times or fail immediately. Also a longer timeout, to allow for the entry of the PIN would be required.

The processing of this transaction may be broken down in to various sub levels depending on which entity will hold and check the PIN number entry and how this information is transported back through the systems. The application on the mobile could simply respond by sending the PIN back to the network for checking at either the Auth Server or at the origination system. I discuss below one of the advantages / vulnerabilities if the same PIN authentication is used for authorising multiple independent systems.

More sophisticated systems could perform digital signatures on the SIM card and return these.

Further study is required in this area to determine the detailed processes of how the PIN is issued, stored, checked and changed. If the PIN is stored and checked within the SIM card then it may be vulnerable to off-line attacks, but if it is stored and checked in the network it needs to be transmitted securely and a robust mechanism implemented to cater for typos in PIN entry.

2.7 Require presence of a secondary Smartcard

This application would prompt with the text for the insertion into the phone of a Smartcard to authenticate the request. This would require that the terminal device had a slot for the card. The card may then ask for a PIN or other verification before sending a response back. This response could either be a simple encoding of the second card number or a full EMV (http://www.emvco.com/) SET (http://www.setco.org/) transaction.

2.8 Require bio-metric verification

This would require the user to place their finger on a print reader or other verification device on their phone to authorise the transaction. Several manufactures are investigating the addition of biometric systems on mobile phones, either as an integrated facility or as a plug in module.

2.9 Location of mobile is within range

The Authentication system will check the mobile is switched on and reporting a current location that is within a range of a location specified in the request message. This might be used when an ATM card is used to check that the users mobile is at the approximate location. This level of authentication might have to deal with inaccuracies in the technologies used to locate the mobile. The user of this system needs to know that they will have to have their mobile with them when they go to the ATM machine.

2.10 Other Levels

Other levels could be added in a transparent manner.

There could be a request to the Auth Server for authorisation at a level that the phone or network was not capable of supporting would return a "not capable" response. There could also be a “Request Capabilities” request that would respond with a string of all the verification levels supported for that mobile / network combination.

Alternatively a directed graph of authentication levels could be defined and the system would attempt to authenticate to the requested level, if this fails then lower levels would be attempted and the requestor returned the highest level achieved. It would then be up to the requesting system to decide whether to accept that level or fail the transaction or access.

The aim would be to make all levels work independently of the mobile being in the home network / roaming network, but it may be that certain capabilities are not available in all networks, so applications using this would need to cater for the "not capable" response.

3. Performance and timing constraints

Many of the applications that could use this sort of authentication system currently use methods that only require automatic responses. This means that these systems are sensitive to long time delays in processing truncations. This is reflected in the range of levels of authentication. Some of the lower levels that do not require user interaction would respond more quickly but with a reduced level of authentication. Higher authentication levels may require longer or require special mobile devices.

I have proposed the use of SMS messaging and applications that could be written in Sim-Tool-Kit so that existing mobile devices could be used for all but the highest levels of authentication. This would mean that such a system could be rolled out and adopted quickly.

4. Uses

I envision a number of uses for such a system. These are my initial ideas.

4.1 VPN and remote system access

A remote user or a local user attempting to access system could be verified. Either this could be done by an authentication server such as used in a Kerbros system or by logon scripts within an application. Many corporate are using systems such as Secure-ID to authenticate users. The user is verified by being able to enter a code from the secure ID tag, thus proving they are in possession of the Secure ID tag. Many of these sorts of users would also have a mobile so proving possession of the mobile would be an equivalent level of security.

4.2 Credit Card Transaction

Rather than trying to do the whole m-commerce transaction on the mobile phone just do the authorisation step. If this were done with digital certificates then this would have the same legal weight as a physical signature.

In card not present transactions the cardholder is verified through knowledge of the CC number and the expiry date on the card. When a fraud is purported the real card holder usually only finds out when they check the card statement. This sort of system would mean that the fraudulent transaction would be stopped immediately. Even if the authentication was using only SMS or USSD messaging, the real cardholder would know of the fraud immediately and hopefully would take action immediately.

Different levels of authorisation could be performed depending on the transaction amount, card present/ not present, the type of retailer involved, etc.

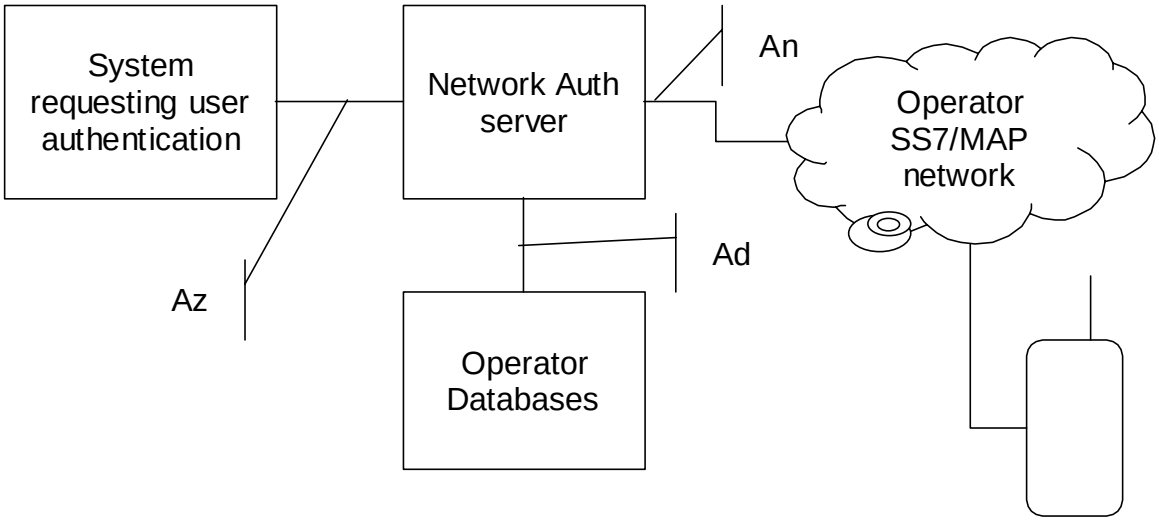
A consequence of sending these messages to the mobile would be that the customer could keep an audit log of all their transactions, this might interface with programs such as Quicken, or MS Money to reconcile bank and credit card transactions. There may be some issues here in the number of these messages that could be stored, and where they are stored, on the phone or the SIM card.

4.3 Internet access to a bank account

Many banks are grappling with the authentication requirements of providing access to account information over the Internet for their customers. I Germany the banks have agreed a specification for a smart card to authorise these accesses, but this requires users to install a smart card reader on the PC they wish to use. The proposed system would remove the requirement for the reader to be fixed to a particular machine allowing access from any internet connected machine such as one in an internet café.

5 What needs to be done next

5.1 Definition of the interfaces



Az Interface

This is the connection to the outside world. This would allow a system that requires authentication to send a "Authentication Request" to request the system to perform an authentication. The idenity od the mobile phone and the adress of the Network Auth Server need to be registered in the originating system. It seems to me that this interface should be an XML interface.

This interface could appear like an credit card issueing bank interface. This would make interfaceing with existing banking systems much easier, though the issue of transporting the MS-ISDN number across this interface would need to be tackeled.

Ad Interface

This is a standard database lookup, response interface. ODBC? SQL?

An Interface

This is an SS7 network interface that will need to send and receive MAP messages to interface with the mobile and other network systems.

6 System Performance

There are a number of performance issues that need to be addressed. The most important the levels that require the delivery of an SMS to the mobile need to achieve this in a matter of a few seconds. For this reason I have proposed not using an SMSC but sending the SMS message directly to the mobile, i.e. the Network Auth Server would act as an SMSC and issue the SS7 MAP commands to send the message directly to the mobile. If USSD messages are used this may simplify the design of the system.

7 System Security and Integrity

The main threat to this system would be over the Az interface. The Network Auth Server would need to have strong method of authenticating systems requiring user authentication. The connection between the systems would need to be encrypted to protect the contents and the integrity of the authentication process.

8 Business Model

A number of business models can be envisioned. The simplest would be that the operator would charge a transaction charge for each authentication request submitted. The amount might vary depending on the level of authentication requested. Inter operator charges would be based on the existing settlement arrangements for SMS message billing. There is no mechanism for inter-operator charging for SS7 MAP messages.

A more sophisticated model might be that the operator gets a percentage of the transaction value for each successful authentication. This would encourage the operator to run a reliable system that would be unlikely to give an authentication failure because of network or system failure.

Operators may wish to offer this service free from transaction charges. Instead getting revenue from related effects of more customers on their network and more calls because customers have their phone turned on and available more of the time so are more likely to use them.

9 Customer Acceptance

New services are usually only accepted by the general public if they see a tangible benefit for themselves. For this reason customer acceptance of security measures are usually only seen as a nuisance because it makes things harder for them to use.

By providing several levels of authentication customers could be educated into using the higher levels in an incremental manner. Start off with simple message delivery and as customer acceptance grows roll out the higher levels of authentication.

If a range of services adopted this system the customer would increasingly benefit from a single method of authentication. While allowing each service to choose the level of verification used. This may become a powerful tool in making the mobile phone the ubiquitous tool of m-Commerce.

10 Vulnerabilities

This authentication system would only be as reliable as the security of the underling GSM network security. If the users SIM card was cloned then provided an attacker also knew the credit card information they could authorise transactions,

they would just need to make sure their cloned mobile was the last one to perform a Location Update to receive the messages.

If PIN numbers are sent in plain text using SMS or USSD messages then these would only be secure as the A5 over the air encryption and would be venerable to false base-station attacks.

We have not seen any significant exploitation of these vulnerabilities within 2G networks, and these are resolved in 3G network standards. The higher monetary values involved may encourage fraudsters to increase their efforts in finding vulnerabilities in mobile networks.

Putting a user's entire authentication in one basket does increase the venerability if that system is compromised. There is the converse argument that centralising authentication has an advantage in that the consequences of compromising that one system for the user has wide implication so they are likely to take better care of it. It is not the same as giving someone you cash card and PIN to get money out of an ATM on your behalf, which we all know people do.

11 Advantages

The proposed authentication system has a number of advantages. It has been designed so that it can be implemented at the lower levels of authentication without any changes to existing retail credit card machines or mobile phone handsets. The only changes that would be requires are in central server systems.

12 Why this is different from other solutions

12.1 PayBox

PayBox is a system developed by Deutsche bank. In this system your mobile number identifies your PayBox account. You give the retailer your mobile number and this is sent to the PayBox system for verification and clearing. The PayBox system checks the validity of the account and then makes a voice call via an IVR system to the mobile, when the call is answered the customer enters their PIN number to authenticate the transaction.

This system is similar in that it verifies the user via possession of the mobile handset (and the associated SIM card) It may be expensive to operate in that the system has to make voice calls to the customer and these could be of a minute or more duration. This will not work well in a roaming situation where the customer is paying for the international leg of the call.

12.2 RSA Secure-ID via SMS

RSA are currently trailing a version of their Secure-ID product where the authentication number is sent to the customer via an SMS message. This then allows them to prove they are in possession of the mobile, by quoting the number sent in the message.

This fine for the specific cases where there is another system that can be used to return the number for checking. So this system would only be applicable to access control to web based systems. RSA state that because of the design of this system it would not be usable for VPN access control. Clearly this could not be used in a conventional shop situation where there is no system for the customer to enter this number.