Voicemail Security Guidelines

Version 2.0

09 July 2020

This is a Non-binding Permanent Reference Document of the GSMA

Security Classification: Non-confidential

Access to and distribution of this document is restricted to the persons permitted by the security classification. This document is confidential to the Association and is subject to copyright protection. This document is to be used only for the purposes for which it has been supplied and information contained in it must not be disclosed or in any other way made available, in whole or in part, to persons other than those permitted under the security classification without the prior written approval of the Association.

Copyright Notice

Disclaimer

The GSM Association ("Association") makes no representation, warranty or undertaking (express or implied) with respect to and does not accept any responsibility for, and hereby disclaims liability for the accuracy or completeness or timeliness of the information contained in this document. The information contained in this document may be subject to change without prior notice.

Antitrust Notice

The information contain herein is in full compliance with the GSM Association's antitrust compliance policy.

Table of Contents

1 Introduction

1.1 Overview

Voicemail systems protect customer Voicemail accounts using two different types of authentication:

Customer authentication, typically using a PIN, and device authentication based on the authentication of the device against the network; for mobile radio networks often using AKA algorithm and secrets in the UICC.

Customer authentication ensures that only the legitimate customer is accessing the Voicemail and is usually used to secure access using a PIN code when device authentication is not possible or not trusted by the mobile network operator e.g. when the customer is roaming or has engaged call forwarding services.

Visual Voicemail systems additionally allow the owner of the Voicemail box to access voicemails using an app on a mobile device. That app also needs to authenticate to the Voicemail box. Such access can be implemented using the IMAP protocol and secured by means of an IMAP username and password.

This document is intended to act as guidance for Operators and Customers in the use of Voicemail PINs that secure access to Voicemail and Visual Voicemail services.

1.2 Scope

This document deals with, and distinguishes between, the following three types of attack against Voicemail systems:

- **Eavesdropping:** listening secretly to the Voicemail content of a particular customer. Voicemail spying is an issue in particular for business customers who may often leave business confidential information on their colleagues' Voicemail assuming it is secure.
- **Fraudulent calls:** breaking into the Voicemail of any customer in order to carry fraudulent calls. Some Voicemail services allow dialling of numbers from Voicemail accounts. For example, the fraudster first leaves a message on the compromised Voicemail from an international or a premium number and then calls back this number through the Voicemail system. This technique allows for the making of fraudulent calls without setting up fake customer accounts.
- **Denial of service:** An attacker might be able to temporarily disable the Voicemail box, preventing the customer from using the service. An attacker might also be able to delete the victim's voicemails, greeting messages, or change their settings, including PIN codes.

1.3 Definition of Terms

Term	Description
CAMEL – Customized Applications for Mobile networks Enhanced Logic	Standard for mobile communication networks that provides extended functionality such as prepaid billing, and also helps to ensure CLI can be trusted
CLI – Calling Line Identity	Where the telephone number calling you is provided and

	displayed on your terminal or device
DTMF – Dual-tone multi-frequency signalling	A telecommunication signalling system using the voice-frequency band; this can be used by a user on his phone to transmit numbers over voice communication lines, for example to enter PINs or to make selections in interactive voice response systems, such as Voicemail systems
HPLMN - Home Public Land Mobile Network	The Public Land Mobile Network that holds the subscriber's profile / that issued the UICC
IMAP – Internet Message Access Protocol	Protocol often used to access Visual Voicemail, see also RFC 3501
ISO/IEC 27000	A family of security standards published by the International Standards Organisation ISO
OMTP - Open Mobile Terminal Platform	Forum created by mobile network operators to discuss standards with manufacturers, e.g. for Voicemail. In June 2010 the OMTP was transitioned into the Wholesale Applications Community, which was closed in July 2012, when GSMA took over the OMTP standards.
PIN – Personal Identity Number	A series of digits randomly chosen to authenticate a Customer
PLMN – Public Land Mobile Network	A public mobile radio network with base stations (as opposed to mobile satellite systems)
PSTN – Public Switched Telephone Network	The conventional telephone system
SMS – Short Message Service	Also known as a text message. A message sent that can be displayed on a telephone
TLS – Transport Layer Security	Used to provide secure communications over an IP (internet protocol) connection
UICC – Universal Integrated Circuit Card	A Smart Card also sometimes known as a SIM (Subscriber Identification Module) used to provide Customer or Device Authentication in Mobile Radio
VM - Voicemail	System that facilitates the recording, storage, retrieval and sharing of personal voice messages
VPLMN – Visited Public Land Mobile Network	The Public Land Mobile Network currently used by the subscriber. VPLMN is different from HPLMN when the user is roaming.
VVM – Visual Voicemail	Voicemail with a visual interface that can support a range of features including presentation of a list of messages for playback, a transcript of each message, etc.

2 Voicemail Authentication

Voicemail systems protect customer Voicemail accounts using two different types of authentication: customer authentication and device authentication.

Customer authentication ensures that only the legitimate customer is accessing the Voicemail and is usually used to secure access using a PIN code when device authentication is not possible or not trusted by the mobile network operator, e.g. when the customer is roaming. The legitimate users may also call their Voicemail boxes from other phones (e.g. when the mobile phone battery is empty) and are still able to listen to their Voicemails.

Device authentication ensures that only a mobile phone with a legitimate UICC is accessing the Voicemail account and is usually used when customers access their Voicemail from their mobile while roaming or from the home network using the calling line number. Typically, device authentication is used on its own when it is reliable (e.g. when CLI can be trusted), so that customers can listen to Voicemails without having to enter a PIN. Customer authentication is used when the device authentication is not reliable.

Other types of device authentication exist that use a username and password that are provisioned in the device over the air and are used to authenticate over a TLS connection such as Visual Voicemail. Authentication is done between the Visual Voicemail app and the backend. When the IMAP protocol is used to access Visual Voicemails, IMAP supports authentication using a username and password.

In the case of mobile phones, ownership of the device with the UICC can be considered sufficient to authenticate the customer for retrieval (and deletion) of Voicemail messages. For fixed-line networks, a PIN is usually asked for in addition. For mobile phones the CLI is considered trusted for calls originating in the home mobile network and optionally for calls originating in other trusted mobile networks (to be decided by the mobile network operator).

The Voicemail PIN used for customer authentication, or generally speaking all authentication secrets that need to be entered by humans, need to be memorable and users must be able to input them easily on their phones. Therefore, the secret used is typically numerical (such that it can be entered on the keypad) and often only 4 or 6 digits long. As the number of possible PINs is limited, the PIN might be guessed and a limitation of PIN entry retries needs to be implemented to prevent brute-force attacks.

Authentication secrets that are automatically transmitted between machines (e.g. between the Visual Voicemail app and the backend) do not need to fulfil these restrictions. Therefore, longer and more complex alphanumerical passwords can be used.

3 Voicemail Vulnerabilities

Voicemail systems can be attacked by exploiting the following vulnerabilities:

- **PIN code guessing:** Some Voicemail PINs can be easily guessed because either the customer chose a very common PIN such as: 1234, 1111, and 2222 or chose a date known to the attacker such as a birthday, or the MNO assigned a default PIN (either constant for all users or based on some scheme the rules of which the attacker can learn) that the customer did not change. If there is only a limited number of potential PINs and no limitation of PIN entry retries, an attacker might try to systematically test all PINs (brute-force attack). A brute-force attack can be carried out over consecutive calls.
- **Visual Voicemail password guessing:** Depending on the implementation, an attacker might also try to guess the password, e.g. if the password used for Visual Voicemail authentication is short and not complex enough, or the attacker might also try to systematically test all possible passwords, or passwords from a word list.

- **Calling line spoofing:** The attacker exploits the fact that some operators provide access to the PSTN without checking whether the calling number belongs to the number ranges assigned to them. This weakness allows the attacker to call the Voicemail of customers of other operators (to which CLI may not be provided, for example on some International Calls) using their calling line number without having to enter the Voicemail PIN. There are web services that offer to make a call with a spoofed CLI by calling back the caller.
- **Social Engineering:** There are many social engineering techniques that can be used to trick or persuade people to disclose information, e.g. tricking customer service staff or customers into revealing Voicemail PINs over the phone.

NOTE: Voice calls might be used as a second authentication factor or as part of an account recovery procedure. Most accounts on the internet are still secured by username and password. For accounts that require higher security, some service providers offer two-factor authentication, where an additional authentication step is required by the user to login successfully. In the past, such services often sent out one-time PINs via SMS. For users that do not have access to a device that is capable of receiving SMS, some of these services also offer automated calls where the service calls the user’s phone and a synthesized computer voice reads the one-time PIN on the phone. If an attacker manages to re-route such a call to the user’s Voicemail box and then manages to get access to the Voicemail box content, he or she may be able to compromise these two-factor authentication schemes. Alternatively, some on-line services call users and require them to enter a one-time PIN via DTMF as a second authentication factor. If an attacker can change the victim’s greeting message to the required DTMF tone then such methods can be compromised too. Some services also use these methods as part of their account recovery procedures. Therefore, if an attacker can retrieve Voicemail messages or change greeting messages to DTMF tones, he may also be able to take over the victim’s on-line account.

NOTE: There are some additional security concerns when Voicemail application servers are virtualized or implemented in a cloud environment. It is beyond the scope of this document to cover all of these topics. GSMA members can find guidance in document FS.33 Network Function Virtualization (NFV) Threat Analysis, available on the InfoCentre[2].

4 Voicemail Security Recommendations for Operators

As is the case with securing any system, it is important that service providers are mindful of the need to ensure an appropriate balance between usability and security. Although the issue of Voicemail security has received a lot of media attention it is important that a sense of perspective is maintained because a few hundred mobile users had their Voicemail messages intercepted whereas several million people use the service with no real concerns about anyone finding out: “they would be late home” or “needed some bread”. For that reason, it is important to keep Voicemail simple and easy to use for the majority whilst allowing users with more sensitive personal or commercial information to protect their messages. The guidance for network operators provided below is designed to achieve an appropriate balance.

This guidance focuses on Voicemail-specific topics and does not contain general guidance on secure architecture design (such as multi-tier architecture and system hardening). Section 4.1 deals with the general Voicemail service, which is accessed using the Telephony User Interface and where authentication using a PIN may be necessary. Section 4.2 focuses on the Visual Voicemail (VVM) service where the VVM password is important. Section 4.3 addresses general topics not specifically bound to general Voicemail or Visual Voicemail.

4.1 Recommendations for General Voicemail Service

4.1.1 Generation of PINs

Each Voicemail PIN should be randomly generated and not derived from any other data or set to a default value. Default PINs should not allow remote access to Voicemail accounts.

If the PIN is derived from some other data, that data must not be known to, or be predictable by, an attacker (such as the MSISDN) and it must have at least some random properties to ensure different users are likely to have different PINs. When using unique identifiers it is preferable to use the least significant digits that change most often as part of derivation.

It is also possible that accounts are not assigned a PIN, or are assigned a default PIN which the user needs to change before being able to authenticate as the legitimate user. In order to authenticate, the user must call from his mobile phone in the home network to set a PIN, or to change the default PIN to a personally chosen. Until a customer chosen PIN is set, authentication using the PIN is not possible.

If users are allowed to choose their own PIN, some basic rules and checks for weak PINs are recommended (e.g. new PIN must not be the same as the default PIN, see also section 4.1.3). Default and/or temporary PINs must be permanently removed.

4.1.2 Length of PINs

PINs should be of variable length of at least four digits but, if possible, mobile users with sensitive information and heightened security needs should be given the option to randomly choose PINs of greater than four digits in length. It is recommended that users are given the possibility to choose PINs with a length of up to 8 digits.

4.1.3 Exclusion of Obvious Patterns

PINs composed of simple repeated numbers or sequences should be excluded. It is recommended that the following PINs should not be allowed: 1234, 1111, 2222, 3333, 4444, 5555, 6666, 7777, 8888, 9999, 0000, and 1212.

Optionally, network operators may wish to allow mobile users that have no security concerns to use easily remembered PINs but advise them against using those PINs for other purposes, such as Banking. The use of easily remembered PINs has the advantage of reducing the number of calls to customer care centres from mobile users needing their rarely used PINs to be reset. However, network operators should advise mobile users that may have greater security needs, due to their occupation or position in the community and the likely sensitivity of Voicemail contents, to use more complex PINs and to avoid obvious sequences like their date of birth, marriage date, etc. as these can be relatively easily found by Internet searches or social engineering. Allowing a choice has the advantage of increasing security awareness as mobile users are prompted to consider their security needs.

4.1.4 Voicemail Service Provisioning Procedures and PIN Transmission

Operators should have robust procedures in place for the distribution, management and provisioning of PINs. Good practice dictates that mobile users should not be able to use SMS to initialise a PIN request. PIN resets should only be sent to mobile devices by SMS or some other separate channel.

It should not be possible for anybody within the network operator, other than the call centre employee who is directly in communication with the mobile user, to reset a PIN and it should not be possible to have a PIN reset on the say so of another call centre employee. Call centre staff should not be able to see Voicemail PINs and systems should merely allow staff to initiate the generation of the PIN and the sending of it to the mobile user’s device. Similarly, PINs must never be given out verbally by customer service staff because such an approach is exposed to social engineering risks.A message can be set in the Voicemail message pre-provisioning preamble to remind or force the customer to create a new PIN.

4.1.5 PIN Entry Attempts

The number of consecutive incorrect attempts that mobile users are permitted before they are locked out of the Voicemail service should be limited to three. The number of attempts should be counted over consecutive calls, otherwise a slow brute-force attack would be possible. After the maximum number of successive incorrect attempts has been reached, mobile users should be required to call the network operator’s customer care centre to authenticate themselves and have their Voicemail PINs reset. Mobile users should still be able to access the Voicemail service only from calls with trusted CLI if PIN authentication is blocked due to too many incorrect attempts, unless the customer has configured their Voicemail to always require PIN entry, even for calls with trusted CLI.

4.1.6 PIN Storage

Infrastructure should securely store both voicemails and Voicemail PINs and not allow them to be easily accessed by technical or other network operator staff or external parties. Standard information security techniques such as the ISO/IEC 27000 family of standards should be deployed on equipment entrusted with the storage of this sensitive data.

4.1.7 Optional PIN Usage

If an operator decides not to mandate PIN usage for Voicemail, the customers should be fully informed of the risks of leaving their phones unprotected and the operator should advise the customers to protect their phones using a device PIN.

Mobile users should not have PIN access to their Voicemail unless they specifically request it for remote retrieval of Voicemail messages. Even then, it may not always be necessary to provide this service and operators should carefully consider whether PINs should be activated if requested and whether CLI access should only be provided on the home network.

The majority of customers will only ever access Voicemail from their own phone on their home network so account or device authentication alone should be sufficient for 99% of customers. Instances of Voicemail compromise arose to a large degree simply because all Voicemail users had retrieval numbers and PINs issued, whether the customers needed them or not. If remote access has traditionally been provided, network operators may wish to consider if this really needs to be enabled for every customer or if it can be disabled as a default and turned on by request.

4.1.8 Accessing Voicemail from a CLI Different from the Mobile User's

Careful consideration must be given to ensuring that appropriate security controls are applied to calls initiated from within the home network and these controls should be distinguished from those required for calls originating from other networks due to the risk that the CLI may be 'spoofed'. In some cases, the mobile user's CLI may not be provided or it may not correspond correctly and this situation can arise when international calls do not provide the CLI or access to Voicemail is attempted from a source other than the mobile user's own mobile device. Network operators should always request a PIN when a call is initiated directly to Voicemail from outside their networks and where the device authentication, such as CLI, is not used.

NOTE Network operators may define the CLI as trusted if (1) the CLI is a valid HPLMN subscriber MSISDN and (2) the relevant call is originated in the home network (HPLMN), or in a CAMEL VPLMN and the call is re-routed by IN to HPLMN. Care must be taken to avoid trusting the CLI from calls that originate in external networks but are forwarded via mobiles in the HPLMN. In the case of VoLTE or VoWiFi calls originating from the home network, care must be taken to ensure that CLI spoofing is not possible within the VoLTE or VoWiFi system if the CLI is to be trusted by the Voicemail platform.

Some customers may require access to their Voicemail from foreign networks and if they have not set a Voicemail PIN prior to travelling a randomly generated PIN should be sent by SMS to them. This PIN should never be visible to customer care staff but the account should be marked with a note that a request for a PIN was made, should the customer query receipt of an SMS with a PIN.

4.1.9 Notification of Attempted Access

If an attempt has been made to access a Voicemail mailbox with the incorrect PIN, the customer should be notified after the second attempt (assuming failure at three attempts). The user is in the best position to decide whether the access was made by them or not and notification could be sent by SMS. If SMS is used, every effort should be made to ensure it is clear to the mobile user that the notification is from the network operator rather than it being a platform to launch a phishing attack or premium rate call back fraud.

4.1.10 Last Access Notification

Where technically possible, when mobile users access their Voicemail service an announcement should inform them when their mailbox was last accessed. This can help users to identify whether somebody else had recent access to their mailbox.

4.2 Recommendations for Visual Voicemail Services

4.2.1 Visual Voicemail Registration, Service Provisioning and Password Transmission

Passwords used to authenticate a Visual Voicemail box should be provisioned securely to the mobile device.

In the past, Visual Voicemail passwords were often provisioned via SMS. Other means like push notifications are also conceivable but regardless of which option is chosen the provisioning payload (including the password) must be protected by encryption.

For push-based Visual Voicemail clients the registration process must also be secured. Messages sent to human users, like one-time PINs, shall be human-readable and sent unencrypted. Out-of-band SMS or push notification payloads shall be encrypted and integrity-protected.

More details about service provisioning can be found in the GSMA Permanent Reference Document TS.46 Visual Voicemail Interface Specification, available for download at https://www.gsma.com/newsroom/resources/ts-46-visual-voicemail-interface-specification/.

4.2.2 Generation of Visual Voicemail Passwords

Each Visual Voicemail password should be randomly generated and not derived from any other data nor set to a default value. PINs should not allow access to the Visual Voicemail account. If users are allowed to choose their own passwords, which is generally not recommended, weak passwords (e.g. too short, words on a word list, etc.) should be prevented. Network operators may choose to periodically refresh passwords.

4.2.3 Password Length

Passwords used to authenticate Visual Voicemail boxes should be at least 8 characters long and alphanumeric. Longer passwords are recommended; see also section 4.2.5 Password Entry Attempts. As the user typically does not have to handle the password, there is no obvious reason to not use long passwords.

4.2.4 Password Transmission

As the IMAP username and password are transmitted over an IP connection, typically over the internet, the transmission should be secured to prevent eavesdropping of the password and of the Voicemail content. Typically, IMAP is used with STARTTLS. Using TLS also has privacy advantages for users in case the IMAP username is created based on the MSISDN, especially when users access Voicemail from a public WiFi network.

4.2.5 Password Entry Attempts

The combination of password length and complexity and an optional brute-force prevention mechanism should effectively avert password guessing attempts. The password should either be enforced to be long (e.g. 16 characters) and complex (alphanumeric, distinguishing lowercase and uppercase letters, also allowing digits and special characters, etc.), or some mechanism should prevent systematic password guessing.

The potential for an attacker to perform a successful brute-force attack against the Visual Voicemail password can be estimated by computing the amount of potential passwords and by measuring / testing how many password entries the Visual Voicemail backend can process in a given time frame (e.g. requests per second). The attacker may use multiple clients to create the requests.

Example: The password is 8 characters long, it is not case-sensitive and consists of letters (26 letters) and digits (10 digits) only. The total amount of potential passwords is $(26 + 10)^8 = 2,821,109,907,456$. If the server processes 1,000 requests per second, testing all passwords will take around 89 years. Assuming that the attacker needs to test half of all passwords before he finds the correct one, the attack will probably take 44 years. However, if the password is one of a word list, the attack may be significantly faster and could be considered feasible. Likewise, if the capacity of the server allows far more than 1.000 requests per second to be processed, the time needed for a successful attack will also decrease.

If the success of password brute-force attacks cannot be excluded, some mechanism should be implemented that throttles the amount of password entries per time (e.g. allowing only one password entry attempt per Voicemail box per second), or temporarily blocks the password entry mechanism for a given Voicemail box after a certain amount of incorrect attempts.

4.2.6 Password Storage

Infrastructure should securely store both Voicemails and Visual Voicemail passwords and not allow them to be easily accessed by technical or other network operator staff. Standard information security techniques such as those described in the ISO 27.000 family of standards should be deployed on equipment entrusted with the storage of this sensitive data.

The Visual Voicemail password should also be stored securely on the mobile device. Current mobile operating systems such as Android or iOS provide mechanisms for secure key storage (e.g. keychain), which should be used.

4.3 Recommendations for Both General and Visual Voicemail Service

4.3.1 Limiting Dial Out and Call Back

Sometimes, Voicemail service offerings can allow mobile users to place a call to anybody that has left a Voicemail message simply by pressing a digit. Capabilities such as this are exposed to fraud and network operators should restrict the ability of mobile users to dial any number from their Voicemail accounts and to call back premium rate or international telephone numbers.

4.3.2 Mobile User Advice

Mobile users should be provided with clear security guidance, both on network operator websites and in written form where possible, on the secure use of Voicemail services. Advice to users should also highlight the possible risks and it should outline the various mechanisms by which Voicemail can be accessed (e.g. via the handset, by calling the handset and pressing certain keys during the Voicemail announcement, by a remote dial-in number, etc.).

In particular, it is important to explain and highlight to mobile users that, where Voicemail systems contain information about “new messages” and “old” or “previously listened to” messages, announcements should be carefully listened to as they could indicate attempts to compromise Voicemail security. In particular, instances where “old” messages that have not been listened to by the mailbox owner could indicate unauthorised access.

Users should also be made aware that Voicemail systems may be part of two-factor authentication schemes (where one-time PINs are read by a computer) or account recovery procedures, all of which increases the value of a Voicemail account.

If embarking on a communications exercise on Voicemail security, network operators could take the opportunity to highlight and provide guidance of additional matters including mobile device locking, backups, SIM locking, recording IMEI details, reporting handset theft, etc.

5 Voicemail Security Recommendations for Users

It is recognised that most mobile users are not particularly concerned about, or have any great need for, Voicemail security. However, it is important that they fully understand the security risks associated with the use of Voicemail services, how they could be exposed to those risks and what they can do to protect themselves. Network operators should offer adequate levels of protection and advice to all customers and the necessary enablers should be in place and on offer for those mobile users that wish to enhance their protection levels. In that regard, the guidance that follows may be useful and informative for mobile users.

5.1 Choosing PINs

Mobile users should choose a PIN that is longer than 4 digits, if this option is available from their network operator, and the PIN should not be one that can be easily guessed. When choosing a PIN the following should be avoided:

- Repeated numbers (e.g. 1111)
- Sequential numbers (e.g. 2345)
- Patterns related to the keypad on mobile devices (e.g. 2580)
- Dates of birth (e.g. 2812 for the 28th of December or 1279 for December 1979) as these can often be found on social networking or other Internet sites.
- PINs that are used for other purposes such as banking.

5.2 Changing PINs

Mobile users that are concerned about protecting sensitive information that may be contained in messages left in their Voicemail should regularly change their PIN as this represents good security practice. Quite aside from routine PIN changes, mobile users should immediately change their Voicemail PIN if they believe it may have been observed or compromised by a third party in any way. Mobile users need to be alert to the fact that their PINs can sometimes be recorded and displayed as ‘Last Number Dialled’ data. Caution should be exercised when accessing Voicemail services and inputting PINs on other mobile devices and phones, (such as PINs recorded on a hotel billing system), as it could be possible for third parties to play back the PIN used at a later stage.

5.3 Alert to Compromise

If somebody unauthorised has listened to a mobile user’s Voicemail messages that person has the option to delete or keep the messages. If messages are retained the Voicemail service will generally indicate that the mobile user has “one saved message” rather than “one new message”. If a mobile user hears the first announcement, followed by a message that it has heard for the first time this could indicate mailbox compromise. Consequently, users should listen carefully and take note of whether messages they are hearing for the first time are classified as new or old/saved.

5.4 Leaving Sensitive Information in Voice Messages

As has been highlighted above, Voicemail systems can be compromised so anybody prompted to leave a Voicemail message for a mobile user should exercise caution in terms of the contents of the message to be left. In particular, those leaving messages should refrain from leaving sensitive information such as credit card details etc. in Voicemail messages.

5.5 Overheard Calls

People should always be conscious of where they are and who may be listening in the vicinity when they make or receive telephone calls, be they to mobile or other telephone users. Calls made from, or received in, public places such as airport lounges and railway stations can be easily overheard and have the potential to divulge much more sensitive information than what could be gleaned from a brief Voicemail message.

5.6 Call Back Risks

Mobile users should be careful when replying to Voicemail messages as systems that allow users to call numbers from which messages originated can be targeted by those seeking to profit from phishing or premium rate call scams. Mobile users should be aware that calling premium rate calls can result in significant call costs and calls from these numbers should not be returned unless the user is satisfied that the message and caller is genuine.Increased Value of Voicemail Boxes

Mobile users should be aware that Voicemail systems may be part of two-factor authentication schemes (where one-time PINs are read by a computer) or account recovery procedures, all of which increases the value of a Voicemail account and thereby also the motivation for attackers. If users provided their mobile phone number to a service which might use that number for purposes such as two-factor authentication or account recovery, users should be careful to protect their Voicemail account adequately, e.g. by setting a PIN which is longer than the default PIN length.

Annex A Document Management

A.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
0.1	11-Nov-11	First draft produced by Charles Brookson	SG Mgt. Team	C. Brookson, SG Chair
1.0	20-Feb-12	First version approved by EMC 2012	EMC	C. Brookson, SG Chair
1.1	12-Dec-14	Transferred PRD from SG to FASG as SG.20 v1.1	FASG	David Chong, GSMA
2.0	09-Jul-20	Document updated to add recommendations on visual voicemail and to generally enhance existing guidance	FASG	Volker Schenk, Deutsche Telekom

A.2 Other Information

Type	Description
Document Owner	FASG
Editor / Company	James Moran, GSMA

It is our intention to provide a quality product for your use. If you find any errors or omissions, please contact us with your comments. You may notify us at prd@gsma.com

Your comments or suggestions & questions are always welcome.