Cell-ID
System Description

Cell-ID: System Description
Document version:1.4

Cell-ID
SMART User Authentication

System Description

Table of Contents

Expertron Group (Pty) Ltd

Tel: +27 (0) 12 349-0390
Fax: +27 (0) 12 349-0360
info@expertron.co.za
http://www.expertron.co.za

Introduction

Cell-ID is a strong, token-based user authentication system that uses possession of a GSM SIM card (effectively the mobile telephone) as an authentication token to authenticate the identity of a person trying to gain access to a computer/network service. When a user logs into a computer-based system protected by Cell-ID, an SMS message containing a random one-time passcode is sent to the user's mobile telephone. This passcode is valid for a limited period of time for only a single and unique authentication session. Cell-ID can also be combined with a password or a PIN for a stronger two-factor authentication mechanism. Cell-ID does not require the rollout of hardware, software or devices to the users who will be authenticated, but assumes that users are already in possession of a mobile telephone with an active, valid SIM card. The SMS delivery mechanism used by Cell-ID can be shown to provide acceptable performance metrics so that Cell-ID can be used as a feasible real-time authentication mechanism.

Cell-ID is secure

A separate, authenticated (GSM) communication channel is used to deliver cryptographically strong one-time passcodes to a user's mobile telephone when logging into a secure service over an IP network. The user is alerted (by an SMS on her mobile telephone) whenever someone else tries to gain access to her account. All authentication events are logged.

Cell-ID is affordable

Cell-ID needs a significantly lower capital investment than competing token-based authentication products (important in an environment where technology is rabidly changing). The total running cost of Cell-ID is less than that of other strong authentication products. Cell-ID spreads the cost of authentication much more evenly over the years of operation, thus limiting the "peak budget"-effect for the first year of operation.

Cell-ID is simple to roll out

No extra authentication tokens for users to carry and no software or hardware to install on client computers. The existing mobile telephone infrastructure is used to manage the "tokens". No costly Public Key Infrastructure (PKI) or other token-based infrastructure to roll out and manage.

Cell-ID is simple to use

Cell-ID uses familiar technology that users are already comfortable with. The user logs in as usual, followed by a prompt to type in the Cell-ID passcode which is received on his mobile telephone about 7 seconds after initiating the authentication process.

Background

There are three fundamental concerns when users of computer-based systems, where these systems consist of client and server computers, gain access to secure services:

A. Authentication of the user (and/or client computer) making use of the secure service. This allows the server to confirm the identity of the user (and/or client computer).

B. Authentication of the server providing the secure service. This allows the user to confirm the identity of the server.

C. Encryption (or secrecy) of the communication channel between the server and the client computer. This may be necessary when a high degree of confidentiality is required such as during a private transaction, or when messages need to be digitally signed.

For reasons identified and discussed later in this section, the first of these three concerns, authentication of the user, is the most challenging.

Users may identify themselves to servers usually by providing a “username” or “user number”. Since usernames and numbers are not secrets, it would be easy for an intruder to pose as another person and gain access to that person’s secure services. To prevent this from happening, the identity of the user must be authenticated. User authentication (proof of identity) can commonly be done in three ways:

What you know: Secrets

If the user can show that he or she is in possession of a secret such as a password, PIN, cryptographic key or certificate that only the real user is supposed to know, it may act as proof of identity.

What you have: Hardware Tokens

If the user can show that he or she is in possession of a hardware device, such as a magnetic card, smart card, cryptographic token or calculator, that only the real user is supposed to have, it may act as proof of identity.

What you are: Bio-metric Measurements

If the user can show that a measurement of part of his or her body (such as a fingerprint, retina scan, photograph, etc.) matches that of the real user, it may act as proof of identity.

User authentication based on a secret, particularly where this secret is a password or PIN that is managed by the user, is generally considered a **weak** authentication mechanism because

- users are known to choose weak (short, easy-to-guess) passwords that can easily be remembered;
- users may write down or share passwords;
- passwords are static; users do not usually change their passwords on a frequent basis, and if the secret “leaks out”, the user can never sure that his or her secret is not known by a third party unless this is changed on a frequent basis.

Authentication based on a secret such as a suitably long cryptographic key (i.e. where decipherment is infeasible) is considered a **strong** user authentication mechanism.

Authentication mechanisms based on hardware tokens are **strong** authentication mechanisms because identity of the user cannot be verified by guessing a secret. Furthermore, the user can be assured that as long as she is in possession of the hardware token, access to her secure services by a third party is impossible.

Authentication mechanisms using bio-metric measurements are also **strong**, since these are not based on a secret that the user knows, and therefore has to remember. However, bio-metric measurements of a particular user do not change (i.e. they are static), and hence, when the measurement is encoded into some electronic format that is transmitted over open communication channels, this information must be kept secret. Hence, these measurements must be encrypted to preserve their secrecy and integrity to prevent unauthorized use by an impostor. In this sense, due to the static nature of bio-metric measurements and their transmission over open channels, these are essentially no different from authentication mechanisms based on strong secrets.

Hence, authentication credentials can either be

- **Static**, such as cryptographic keys that must be installed on computing equipment (both client and server); passwords that users must remember; measurements of bio-metric entities such as fingerprints, retinas, voice, etc;

- **Dynamic**, such as one-time passwords (OTP) generated by some hardware token, where possession of the token, and hence identity, is proved by offering the OTP. One-time passwords may either be generated by algorithmic processes based on some cryptographic key, or generated by random processes.

Dynamic credentials provide a significant advantage over static credentials: with dynamic authentication credentials, the validity of a one-time password for a particular authentication session expires after some time, and even if the password does “leak out” it cannot be used for future authentication sessions. Furthermore, depending on the authentication protocol, it may even be infeasible for an impostor to use a “leaked-out” password for a current authentication session: the session must be hijacked since a different password is generated for each new authentication session.

All existing strong methods of authenticating users suffer from two practical problems:

The Distribution Problem

The *distribution problem* refers to the difficulty of “rolling out” the user authentication technology. In all cases, either secret keys, hardware tokens such as cryptographic tokens and calculators, software programs or devices such as card readers and biometric scanners must be distributed to all the users. Usually there are many more users than servers, and where the servers may be centrally located, users are usually widely distributed. This creates logistical problems where, due to the difficulty of distributing the necessary software and/or devices to the users, the implementation of strong authentication systems is, in many cases expensive and impractical. This is particularly the case where the user base is large, for example, where users from among the general public make use of online Internet subscription services including, but not limited to, Internet banking, access to electronic media and literature, insurance services, stockbrokerage, investment and other financial services, health services, as well as other online technologies such as e-commerce, submission of electronic forms such as for tax returns, etc.

The Registration Problem

All strong user authentication mechanisms use a database to match usernames or numbers with a cryptographic key, retina pattern, hardware token serial number, etc. The *registration problem* refers to the difficulty in populating the authentication database with correct information. If the initial registration of information into this database is not a trustworthy process, the security of the authentication mechanism is compromised. The registration problem is particularly evident when users from a large user base, such as from among the general public, need to be authenticated for online services such as those listed in the above paragraph. An outstanding feature of any authentication mechanism, particularly for Internet applications, is the ability to authenticate users who have not yet registered for the authentication service, or at least to enable the user to register online in order to make immediate use of secure online services.

For large, widely-distributed user bases making use of publicly-accessible, secure computer-based services which are centrally located, strong user authentication is a challenging problem to solve. Strong authentication of **servers**, especially where these servers are few and centrally located, can be solved in a practical and secure way by existing methods that are not affected by the distribution and registration problems. These methods typically utilize technology based on public-key cryptography (such as SSL), where public keys located on servers provide both strong authentication of the server to the user, as well as secrecy (encryption) during the transaction. However, there still remains the residual problem of implementing practical, strong user authentication.

The Cell-ID system was designed to provide strong user authentication in a practical way by using mobile telephones as identity authentication tokens. It solves the token rollout problem by using the existing mobile communication infrastructure. It assumes that the majority of users who need to be authenticated are already in possession of a mobile telephone. Furthermore, Cell-ID could also make use of existing trusted databases containing username and mobile telephone number pairs during the authentication process.

An authentication mechanism, such as Cell-ID, which makes use of existing infrastructure, such as hardware tokens and databases, is particularly suitable for applications that require strong authentication of users from large user bases, such as from among the general public.

Cell-ID Applications

Cell-ID provides a practical way to authenticate the identity of users of computer systems for applications including:

Dial-up Remote Access

Many organizations require that internal and/or external support personnel must have direct, remote access to mission critical systems, minimizing downtime and cost-to-reaction for servicing core business system. Hence, remote dial-up access (RAS) must allow a user direct access to sensitive systems that reside on the corporate LAN/WAN. Since dial-up access is usually only protected by a username and a weak password, potentially anyone who has access to a modem may attempt a break-in to this vulnerable portal to the network, and if successful, may have full access to mission critical systems. Hence, for roaming users, strong user authentication is critical.

Cell-ID uses a standard RADIUS (Remote Authentication Dial In User Service) interface to authenticate dial-up user access via a NAS (Network Access Server), supporting standard RADIUS features such as dial-back. Cell-ID can also be integrated, via the RADIUS Authentication Proxy, with CiscoSecure, leveraging additional security features offered by the Cisco investment.

Operating Systems

Cell-ID can be used to authenticate access to the operating systems of enterprise UNIX computer systems via Telnet, RLOGIN, RSH, and X-Windows. Cell-ID makes of a standard interface called PAM (Pluggable Authentication Modules) to authenticate users.

Application Software

Cell-ID can be used to authenticate access to applications and services such as FTP and HTTP (Web).

Firewalls

Through a standard RADIUS interface, Cell-ID can be used to authenticate access through firewalls via application proxies that support RADIUS authentication.

Web-based Online Internet Subscription Services

Cell-ID can be used to authenticate users who make use of Web-based Internet subscription services such as Internet Banking, Investment Portals and other financial services, online Medical Scheme services, online Insurance and Stockbrokerage services, and Electronic Media and Literature.

e-Commerce

For online Credit Card transactions, where credit card issuers will not accept the risk of fraud and charge losses back to the merchants, authenticating the identity of the person conducting the transaction provides an important business advantage. Cell-ID can be used to reduce the fraud associated with on-line transactions by linking the identity of a person with his/her credit card number in a "strong" way for every transaction. Furthermore, Cell-ID can also be used to digitally sign the contents of a transaction so that an authenticated user can be associated with a specific transaction.

Figure 1 shows common applications for the Cell-ID authentication system. The Cell-ID icons indicate services that can be Cell-ID protected. Cell-ID can also be integrated with CiscoSecure through its standard RADIUS interface.

It is possible to license the Cell-ID system either

- as a complete, stand-alone system (hardware, software and license), or
- as a centralized authentication service (license only), providing a centralized authenticating resource for authenticating users for any of the above-mentioned services.

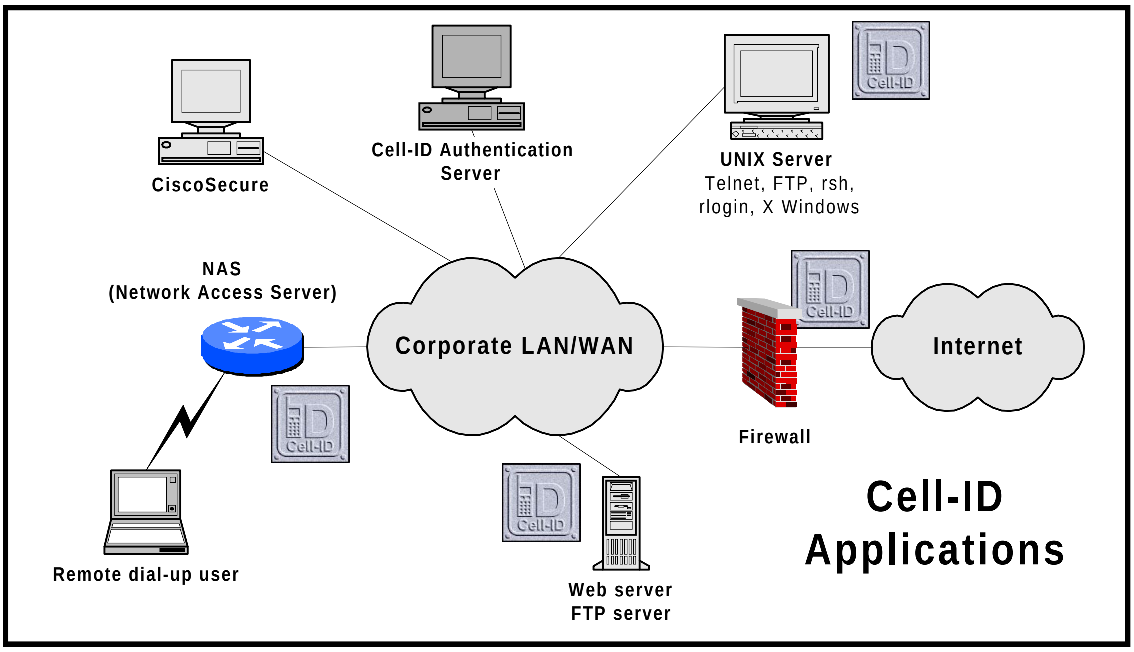

Figure 1: Cell-ID applications

Cell-ID Authentication Process

The following two steps embody the Cell-ID Authentication Process:

A. User Registration

The user's details, including (but not limited to) a username or number and his or her mobile telephone number are registered in the Cell-ID user database. For employees of a company, this can be done by the Cell-ID system administrator and does not need confirmation from third-party sources outside the company. For online Internet services where users from among the general public can register online, the details submitted by the user to the database must be confirmed by another source. This can be done by asking the user to fax and/or post information such as mobile telephone account statements, credit card statements, etc, and/or by querying other databases such as those from mobile communication network service providers and banks. Every time the information is confirmed, the confidence level, a numerical value reflecting the integrity of the confirmation method, is adjusted and updated in the database.

B. Authentication procedure per login session

The procedure that is performed each time a user logs into a Cell-ID protected system is shown in Figure 2. The following terms will be used in the explanation of Figure 2 that follows:

IP Server

The computer system which provides a secure service over an IP (Internet Protocol) network to which users want to gain access.

Cell-ID Authentication Server

A centralised computer system that performs most of the Cell-ID authentication process. The Cell-ID Authentication Server may provide an authentication service to many IP Servers.

Cell-ID User Database

The Cell-ID User Database contains information matching username (or number) and mobile telephone number pairs. The Cell-ID User Database can be populated by an administrator, or by the users themselves. When users are allowed to register on the Cell-ID User Database, the correctness of the information must be confirmed from third party sources such as databases of mobile communication network service providers, banks or any other trustworthy source of information.

Thin Cell-ID Authentication Clients

Software installed on every IP Server that makes use of the Cell-ID authentication Service. The Thin Client redirects the authentication process (which otherwise may have taken place on the IP server itself) to the Cell-ID Authentication Server.

Cell-ID One-Time Passcode

A random number that is sent from the Cell-ID Authentication Server to the user’s mobile telephone. The user reads the one-time passcode received by his mobile telephone and offers it as a pass-phrase to gain access to secure service(s) offered by the IP Server. The random number is cryptographically strong (generated in hardware), and is used once only for a single, unique login session. The one-time passcode is valid for a limited period of time.

Session Number

Every authentication session is numbered with a (pseudo unique) number, the Session Number. When the Cell-ID Authentication Server sends a message containing the passcode via the mobile communication network to the user’s mobile telephone, it also includes the Session Number. The Thin Authentication Client uses the same session number when prompting the user for the One-Time Passcode. This enables the user to match the received One-Time Passcodes with the correct login session.

Confidence Level

A value associated with each user in the Cell-ID User Database that reflects the integrity of the procedure used to register the user’s details in the database. This value may be updated from time-to-time whenever the user’s registration details are re-confirmed. This value may or may not be used during the authentication process.

The procedures shown in Figure 2 are explained as follows (numbers correspond to those in the figure; lines in red represent encrypted communication channels):

1. The user requests access to a secure Internet service provided by an IP Server (e.g. a Web server) by sending a username or number to identify herself.

2. The IP Server runs a Thin Cell-ID Authentication Client that re-directs the authentication request to the Cell-ID Authentication Server by sending the username and server name or address to the Cell-ID Authentication Server.

3. The Cell-ID Authentication Server generates a random number (the Cell-ID One-Time Passcode) and Session Number, queries the Cell-ID Database for the user’s mobile telephone number and sends a message to the user’s mobile telephone containing the passcode and session number. The message can be sent via SMS, USSD, GPRS or any

other suitable mechanism. The One-Time Passcode, Session Number, as well as a Confidence Level are sent to the IP server (also referred to as the Cell-ID Authentication Client).

4. The user reads the random number from her mobile telephone and offers it via the IP network to the IP Server as a passcode. Note that the Session Number is used to link every Cell-ID message that arrives on the mobile telephone to a specific authentication session.

5. The IP Server compares the random number received from the Cell-ID Authentication Server to the passcode submitted by the user for that particular authentication session. If the two numbers match, the user is granted access. If the numbers do not match, or if a response is not received within a certain time interval, access is denied. The server may also use the Confidence Level (which reflects the confidence of correctness of the user's data in the Cell-ID database) from the Cell-ID Database to determine whether or not the user is granted access.

6. The outcome of the access attempt is sent back to the Cell-ID Authentication Server and logged in the Cell-ID Database.

All actions are logged. This may provide a form of non-repudiation: a person would not be able to deny that he or she used a certain on-line service if access to that service was granted after providing, within a limited period of time, a passcode that was sent to his or her mobile telephone during a period for which the mobile telephone was not reported missing.

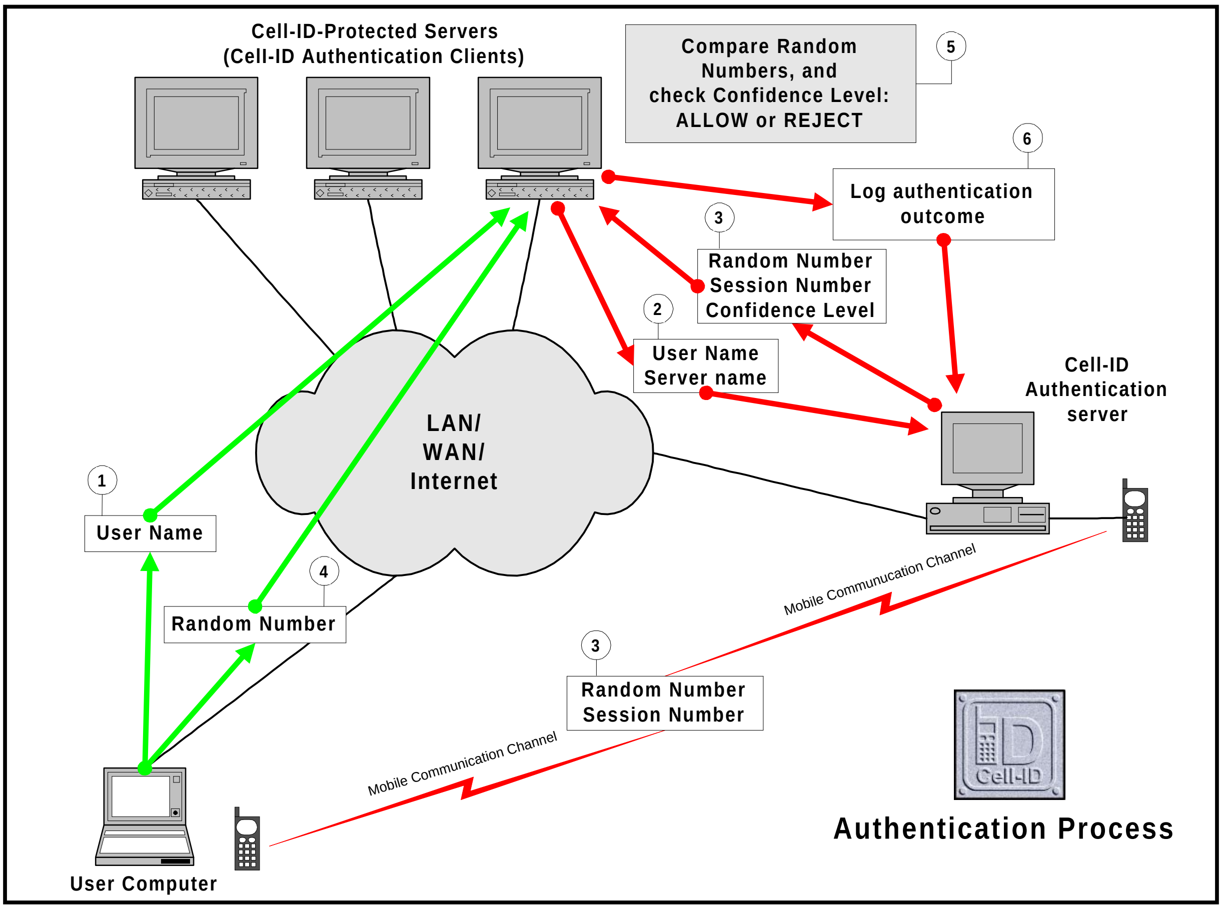

Figure 2: Cell-ID Authentication Process

System Specification

The Cell-ID system comprises hardware and software, both designed for security and reliability.

Cell-ID Server Hardware

Cell-ID server hardware has been designed with ultimate reliability in mind. Industrial specification components are used. To increase reliability further, it is possible to configure two Cell-ID authentication servers in a dual peer-to-peer configuration with hot-takeover capability. If the primary authentication server is down or not reachable via the network, the secondary authentication server is automatically used.

Two Cell-ID models are available. These differ in terms of the reliability of the hardware used for the authentication server. Both models come standard with a single GSM modem which may serve as a backup GSM link for the delivery of SMS messages in the event that the IP link, which is used as the normal channel for SMS delivery, becomes unavailable. For applications that do not require high throughput of SMS messages, or where a direct IP link to the SMSC is not possible, the modem may be used as the primary SMS delivery channel. In this case, it is possible to connect an array of up to 32 modems to a single Cell-ID authentication server for greater throughput and reliability.

Standard Model

- 19" rack-mount chassis.
- 10/100 Mbps Ethernet port.
- Hot-swappable hardware RAID-1 (SCSI) for data integrity and availability.
- Hot-swappable dual-redundant industrial power supply.
- One GSM Modem (expandable up to 32).
- Intel architecture with hardware random number generator.

Small Business Model

- 19" rack-mount chassis.
- 10/100 Mbps Ethernet port.
- Hot-swappable hardware RAID-1 (IDE) for data integrity and availability.
- Single industrial power supply with 204 100 hours MTBF (more than 23 years).
- One GSM Modem (expandable up to 32).
- Intel architecture with hardware random number generator.

Cell-ID Software

The Cell-ID authentication system software comprises the Cell-ID authentication server software, and authentication client software that allows Cell-ID to be used to protect a variety of applications on various platforms.

Cell-ID Authentication Server

The core of the Cell-ID authentication server software is the Cell-ID Authentication Engine. The Engine is highly optimized to service authentication requests and dispatch GSM messages (SMS's in this case), using multiple, redundant dialer queues for speed and reliability. The Cell-ID user database is managed via a Web browser over an SSL-encrypted link. This leverages the use of a standard and familiar interface for operations personnel. The Cell-ID authentication server also includes a RADIUS server that offers a standard authentication interface to many applications. Thus, the Cell-ID server software comprises the following components:

- Hardened (secured), Linux Operating System.
- Cell-ID Authentication Engine.
- MySQL database.
- Cell-ID Database Administration Software.
- RADIUS server.

Authentication Clients

Cell-ID authentication client software enables various applications to make use of the Cell-ID user authentication service. Where these clients interface directly with operating systems, a standard authentication interface called PAM (Pluggable Authentication Modules) is used. Authentication clients for the following popular applications are currently available:

Application	Operating System
Telnet (uses PAM interface)	Solaris (2.6 and up), Linux, BSD
FTP (uses PAM interface)	Solaris (2.6 and up), Linux, BSD
Login, rsh, rlogin (uses PAM interface)	Solaris (2.6 and up), Linux, BSD
X-Windows: dtlogin (uses PAM interface)	Solaris (2.6 and up)
ReflectionX	Windows 95/98/NT
Web server (uses standard module interfaces)	UNIX (Apache), Windows NT/2000 (Apache and IIS)
Dial-up for remote access (uses RADIUS)	Any NAS (Network Access Server) supporting RADIUS

Documentation

- Installation manual (Authentication Clients)
- Administration Manual (Authentication Server)
- User manual (Authentication Server)

Security Features

The Cell-ID authentication server incorporates the following security features:

- **One-Time Passcode.** Every passcode is used once only. Stolen passcodes cannot be used to set up a new connection from any other computer.
- **Hardened Linux Operating System.** Particular care has been taken to ensure that this reliable, trusted operating platform has been securely "bolted down." The Cell-ID server has been designed to operate as a "black box", with no need for operations personnel to gain access to the actual operating system.
- **Encrypted communication links.** All communication links between Cell-ID authentication clients and the server are encrypted. The Cell-ID protocol also embodies mechanisms to protect against Man-in-the-Middle and Replay attacks. The link between two Cell-ID servers in a peer-to-peer configuration is encrypted (with IPSEC), and management of the Cell-ID database is executed via a browser over an SSL-protected link.
- **Logs for Audit Trails.** No security system is complete without detailed logs of all events. The Cell-ID server logs all modifications made to the database, whether made by administrators and operators. These logs cannot be changed or tampered with – even backups of the entire database, and hence the logs, are tamper proof. Furthermore, all authentication events are logged. For each login attempt, the outcome, and reasons for the outcome, are recorded.
- **Real random numbers.** To generate random numbers that truly are random, as opposed to numbers that are only pseudo-random, all passcodes are generated in hardware, and do not rely on a vulnerable pseudo-random software process.

Reliability Features

The Cell-ID authentication server incorporates the following reliability features:

- **Industrial specification hardware.** A robust industrial chassis (with lockable front panel and ball-bearing cooling fan) and industrial power supply respectively house and power the Cell-ID authentication server.
- **Redundant hot-swappable components.** Hard disks are dual-redundant and hot-swappable (RAID-1) for both Cell-ID server models. In the case of the Standard Model, the power supply is also dual-redundant and hot-swappable.
- **Redundant SMS delivery channels.** Both Cell-ID server models come standard with a GSM modem which may be used as a backup GSM channel for SMS delivery in the event of a failure of the direct IP link to the SMSC (SMS server). Furthermore, an array of up to 32 GSM modems may be configured for throughput and reliability.
- **Redundant Cell-ID servers.** It is possible to configure two Cell-ID authentication servers in a dual peer-to-peer configuration with hot-takeover capability. If the primary server is unavailable, Cell-ID authentication clients automatically use the secondary server. All database changes made on any one of the authentication servers are replicated to the other server.

Figure 3 shows the components of the Cell-ID reliability model as discussed above.

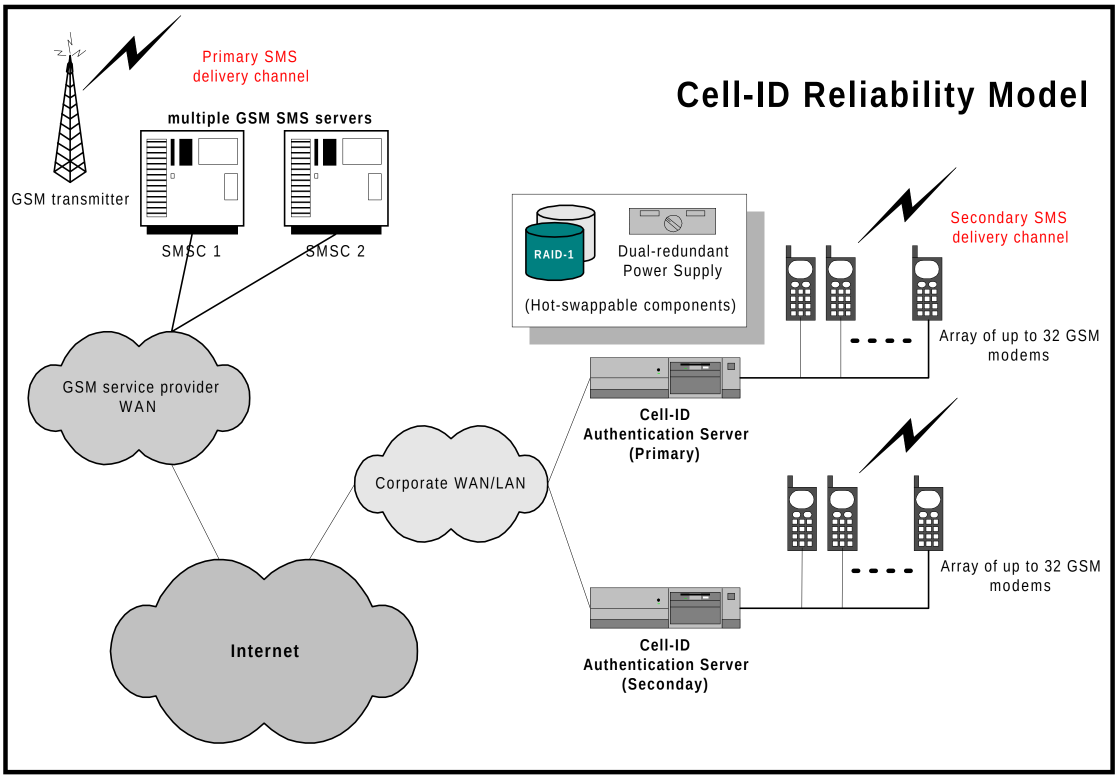

Figure 3: Cell-ID Reliability Model

Performance Issues

The Cell-ID system currently uses SMS to deliver the passcode message to the user's mobile telephone. In Figure 2, it is suggested that SMS messages are sent from a GSM modem directly connected to the Cell-ID server. However, it is preferable to deliver the SMS via a direct IP link to the SMS server (SMSC) of the GSM network service provider. This increases reliability and total throughput (up to 10 SMS messages per second per IP link).

The most critical component affecting the performance of the Cell-ID authentication system is the performance of the GSM message delivery channel between the Cell-ID authentication server and the user. The Cell-ID authentication system is a real-time authentication mechanism, and hence, rapid and reliable delivery of SMS messages is essential. This implies both the throughput of SMS delivery between the Cell-ID authentication server and the SMSC, and the SMS delivery time to the user. Cell-ID places an additional loop around the current SMS delivery protocol (SMPP), and queries the SMSC after 15 seconds to determine whether the first SMS was delivered. If not, the undelivered SMS message is cancelled, and a new one is sent.

Throughput of SMS messages via the IP link is up to 10 messages per second per link (multiple links can be utilized if necessary). The median for SMS message delivery is 6.8 seconds (taken over 300 samples, as shown in Figure 2). Further statistics that can be derived from these trials are (in the graph below, an error is the case where an SMS is delivered after 45 seconds):

Median:	6.82 sec
Average:	7.6 sec
Standard Deviation:	3.47 sec
Maximum:	32.62 sec
Minimum:	5.33 sec
Errors:	2.7 %

Table 1: SMS delivery statistics for direct IP link to SMSC

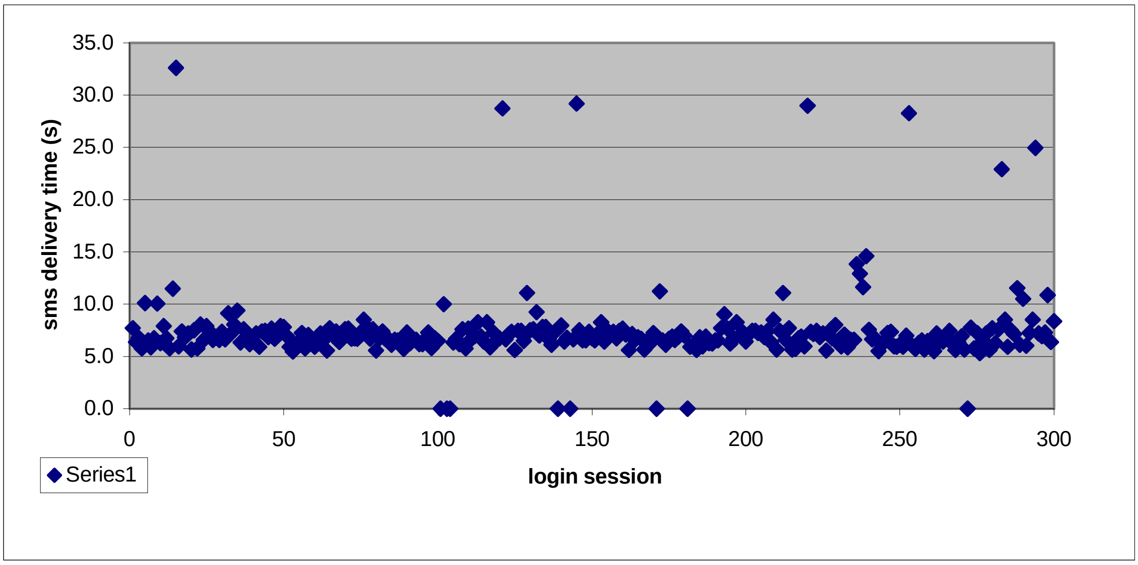

Figure 4: SMS delivery time via direct IP link to SMSC (zero value indicates network error)

Throughput of SMS messages from the GSM modem is approximately five SMS deliveries per minutes per modem (one every 12 seconds), where multiple modems can be configured if necessary. The median for SMS delivery time to the user is 13.7 seconds (taken over 110 samples, as shown in Figure 5). Further statistics that can be derived from these trials are:

Median:	13.67 sec
Average:	13.9 sec
Standard Deviation:	1.90 sec
Maximum:	26.09 sec
Minimum:	11.37 sec
Errors:	4.5 %

Table 2: SMS delivery statistics for GSM modem

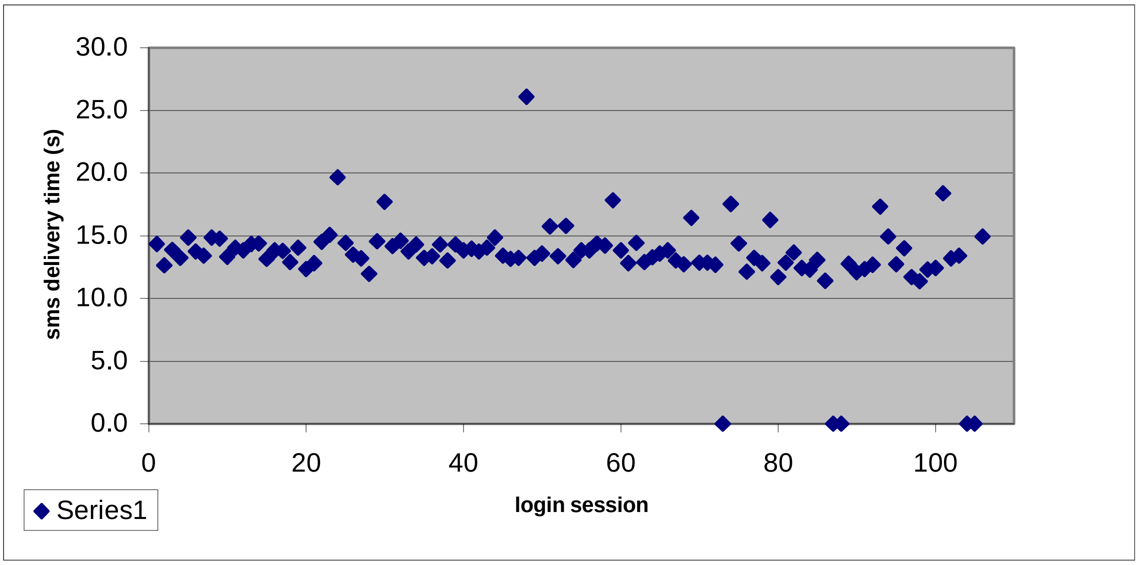

Figure 5: SMS delivery time for GSM modem (zero value indicates network error)

Cell-ID is SMART user authentication

Cell-ID is Secure

A separate, authenticated (GSM) communication channel is used to deliver cryptographically strong one-time passcodes to a user's mobile telephone. The user is alerted (by an SMS message on her mobile telephone) whenever someone else tries to break into her account. All authentication and administrative events are logged.

Cell-ID is Manageable

An SSL-protected web browser interface is used to manage all users and servers from a central database. Cell-ID has an access control feature that makes it possible to enable or disable user access to multiple servers from a single point (useful when an employee leaves a company). No extra authentication tokens for users to carry and no software or hardware to install on client computers. Existing cell-phone infrastructure is used to manage "tokens". The user logs in as usual, followed by a prompt to type in the Cell-ID passcode, which is received on the user’s mobile telephone about 7 seconds after initiating the authentication session.

Cell-ID is Affordable

The total running cost of Cell-ID is less than that of other leading strong authentication products. Cell-ID needs a significantly lower capital investment than competing products (important in an environment where technology changes very fast). Cell-ID spreads the cost of authentication much more evenly over the years of operation, thus limiting the "peak budget" effect for the first year of operation. No costly Public Key Infrastructure (PKI) or token-based infrastructure needs to be rolled out and managed.

Cell-ID is Reliable

All Cell-ID models use industrial computer components. The standard model includes a hot-swappable RAID-1 configuration, with a hot-swappable dual power supply. A peer-to-peer capability eliminates a single point of failure. Redundant SMS delivery channels are used.

Cell-ID is Trustworthy

Cell-ID uses existing technology in a novel way to deliver hard-core security that is associated with other proven and trusted token-based authentication mechanisms that utilize a one-time passcode.

Frequently Asked Questions

What happens if the user's mobile telephone is lost or stolen?

Cell-ID takes advantage of the reporting and change control mechanisms that are already offered by the mobile telephone service providers. Should the user's mobile telephone be lost or stolen, there is already an incentive and a mechanism for the user to have the SIM card blocked as soon as possible. Cell-ID can also be combined with a conventional password, so that if the handset (i.e. the token) is stolen, the criminal would also have to know the password to break into the user's account. The Cell-ID status of the user can also be disabled until the user's handset is replaced, so that the user falls back to her password in the interim.

What happens if I don't have my mobile telephone with me?

Cell-ID is a token-based authentication system, i.e. the user must be able to show that she is in possession of the token: this inconvenience is also the user's protection. However, in contrast to other types of token-based systems, there is already an established bond between a user and her mobile telephone as this device already has other valuable uses. The chance of this not being present when the user wants to access her secure Internet services is less likely than with the case where she must carry around an extra authentication token (such as a smart card or cryptographic calculator).

What happens if the GSM network is down?

In the unlikely event that the GSM network is down, a Cell-ID operator can disable Cell-ID for a particular user, groups of users or all users. The user will then only be required to offer his password (for the case where Cell-ID is normally combined with a password for a stronger two-factor authentication) to gain access to his secure service. The outage of the whole, or part of the GSM network has immense implications for the GSM service providers, and the probability of such an event actually occurring is comparable to failure of the rest of the communication infrastructure around the secure Internet service (e.g. fixed-line operators, ISP's, etc).

How reliable is SMS?

SMS is becoming big business for the mobile telephone service providers. This service is also used for various mission-critical systems such as vehicle tracking and recovery. Hence, service providers invest heavily in SMS technology to enhance reliability and performance to migrate SMS from a best-effort notification system to a real-time messaging service. Furthermore, test results in the above section (Performance Issues) show that SMS delivery is reliable and fast. In the near future, Cell-ID will make use of USSD when it becomes available. This GSM messaging service will transmit text messages at the speed of setting up a normal mobile call.

What is USSD?

USSD (Unstructured Supplementary Services Data) is a GSM text messaging service (like SMS), but is not store and forward like SMS, and does not offer retries. Hence, USSD should achieve many times the speed of SMS due its simplicity and much reduced reliance on non-volatile storage, i.e. there is no intermediate SMSC where undelivered messages are queued, since USSD messages are delivered directly to the handset with the speed of setting up a GSM call. USSD is ideal for Cell-ID, as the real-time demands of Cell-ID on the messaging service would not benefit from the delays incurred by a store and forward system.

Doesn't Cell-ID just add unnecessary complexity that will simply discourage users?

There is always a compromise between security and convenience – security is designed, after all, to restrict access by keeping unwanted users out. Cell-ID is a good compromise between these two metrics, offering the hard-core security of a token-based system, whilst utilizing a well-adopted technology that is already familiar to the user.

What if not all users have mobile telephones?

There are over 6 million mobile telephones and 2.2 million Internet users in South Africa (at end of year 2000). Hence, the overlap between Internet users (especially those making use of secure Internet services such as Internet banking) and mobile telephone owners is quite substantial. It makes sense that a security system should be designed for the norm, and not for the exception. Furthermore, Cell-ID can be offered as a differentiated service to those who own mobile telephones and want the security that Cell-ID offers.

What about other authentication mechanisms that use a one-time passcode generated by the mobile telephone?

Cell-ID is not the silver bullet to solve all the challenges and requirements (security, cost and convenience) of a strong user authentication system – there will never be, and even if so it may yet be way in the future. Cell-ID is solution that works NOW, irrespective of the user's mobile telephone and SIM card since no special SIM card or handset features are required. Solutions that make use of on-card or built-in handset functionality have yet to be rolled out at great expense. Cell-ID is a good, cost-effective intermediate solution that will form a bridge between the present and the future, when it is likely that all authentication will be performed via the user's mobile telephone using built-in handset-specific functions.

How secure is the SMS transmission channel?

The GSM standard dictates that the RF (Radio Frequency) link from the GSM base station to the handset carrying the SMS is encrypted. This would make it highly impractical, and therefore unlikely, for an intruder to intercept the encrypted SMS and decrypt the message within the short time window within which the Cell-ID passcode is valid.