White Paper

Bearer Independent Protocol (BIP)

Giesecke & Devrient

Contents

1 Executive summary 4

2 Introduction 5

3 Solution description 5

3.1 Standards compliance 5

3.2 Interface architecture 6

3.3 Data carriers 9

4 Terminal support 10

5 Service request initialization 11

5.1 Application initiated service request 11

5.2 Server initiated service request 11

6 Service development 12

6.1 Application download and file management 12

6.2 Description of a typical procedure 14

6.3 User information retrieval 16

7 Summary 17

8 Glossary 18

9 About Giesecke & Devrient 19

1 Executive summary

New over-the-air technologies like the high performance communication Bearer Independent Protocol (BIP) will deliver broadband-like data speeds to the (U)SIM. That will enable operators to deliver revenue generating services much faster, more effectively, and with higher reliability than via today's SMS channel.

BIP allows (U)SIM cards to download data through a phone's high speed data channel like GPRS, and 3G onto the (U)SIM. Services like Remote File Management (RFM) or Remote Application Management (RAM) will be significantly faster through BIP and are therefore ideally suited for highly performing administration (e.g. loading, updating) of applications on the (U)SIM.

Larger memory (U)SIMs allow more personal data and lager applications to be stored on the card. Management of the data and applications is significantly improved and made considerably easier and experiences a boost in efficiency with the use of a high speed communication channel, which offers, for example, efficient over-the-air phone book backup, to end customers.

As a result, operators benefit from higher customer satisfaction, reduced customer churn, and, in turn, increased ARPU. On top of this and with the diversified service offering for their subscribers, operators can increase customer loyalty. These possibilities are not merely pie in the sky. The pieces are there now and ready for operators to deploy.

2 Introduction

The Bearer Independent Protocol is a mechanism by which a mobile phone provides a (U)SIM with access to the data bearers supported by the mobile phone (e.g. Bluetooth, IrDA, etc.) and the network (e.g. GPRS, 3G, etc.). This white paper provides a generic overview of bearer independent file management and application download to a (U)SIM card.

3 Solution description

3.1 Standards compliance

Due to G&D's involvement in standardization bodies related to SIMs and (U)SIMs, we are in an excellent position to ensure adherence to the relevant specifications and to anticipate trends in this field. Within the context of BIP solutions, the following specifications and standards must be observed:

ETSI TS 102 223	Smart Cards, Card Application Toolkit (CAT)
Related standards:	
IETF RFC 793	Transmission Control Protocol (TCP), DARPA Internet Program Protocol Specification
ETSI TS 102 124	Smart Cards; Transport Protocol for UICC based Applications; Stage 1
ETSI TS 102 127	Smart cards; Transport protocol for CAT applications; Stage 2
ETSI TS 102 223	Smart Cards; Card Application Toolkit
ETSI TS 102 225	Smart Cards; Secured packet structure for UICC based applications
ETSI ST 102 226	Smart Cards; Remote APDU structure for UICC based applications
3GPP TS 23.048	Specification of security mechanisms for the SIM Application Toolkit, Stage 2
3GPP TS 31.115	Secured packet structure for (U)SIM Toolkit applications
3GPP TS 31.116	Remote APDU Structure for (U)SIM Toolkit applications
3GPP TS 31.111	Specification of the USIM/SIM Application Toolkit for the SIM/ME interface

3.2 Interface architecture

G&D has already developed several different card implementations for BIP as part of the G&D initiative for high bandwidth communication. Clearly, BIP has been designed to make use of any IP based connection the phone is capable of establishing (e.g. GPRS or 3G).

CAT_TP versus TCP

The transport protocols described are independent of applications and bearers being used. The protocols guarantee the data transmitted from is received intact and in the exact sequence in which it was sent.

CAT_TP is a transport protocol specified solely for usage in the (U)SIM ⇔ server context. The corresponding CAT_TP specifications were released by ETSI (please refer to 3.1 Standards compliance).

The CAT_TP protocol allows a data channel to be established by the (U)SIM through the mobile phone to a remote server in the network. Data between the remote server and the mobile phone is exchanged via User Datagram Protocol (UDP). UDP in itself does not provide the assurance of data integrity and sequential transmission that TCP does; datagrams may arrive out of order or go missing without notice. That is why CAT_TP as a backup for the unreliable UDP to ensure acknowledgement, segmentation/fragmentation, retransmission of messages, etc., and stretches from the (U)SIM to the server. It must be implemented on both the (U)SIM and the server.

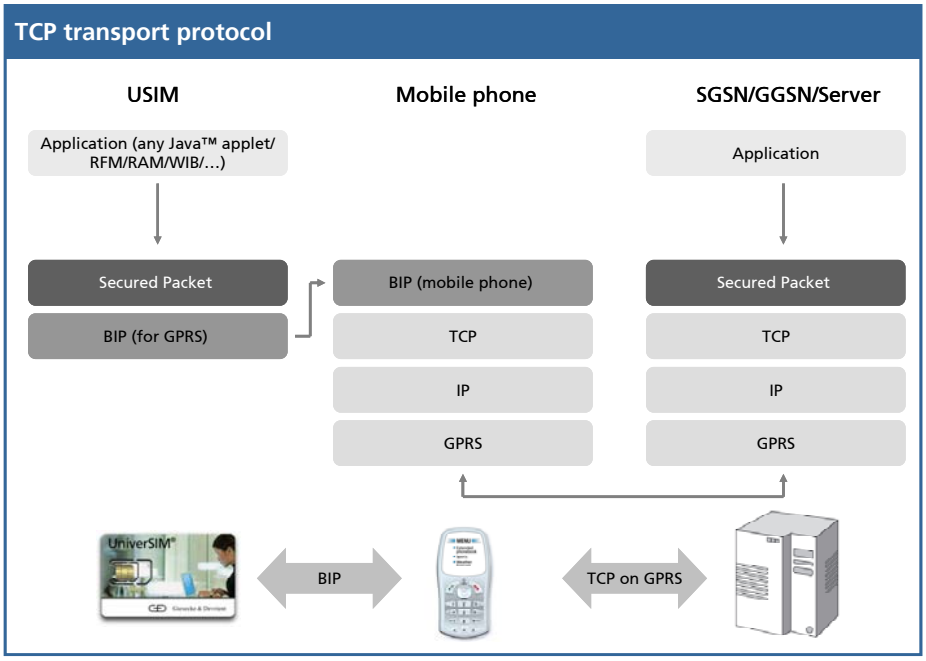
A competing technology is the Transmission Control Protocol (TCP). Traditionally, TCP has been implemented on mobile phones for exchanging data between a WAP server and WAP browsers. The (U)SIM takes advantage of the TCP secured connection between the mobile phone and the server to send and receive data. The corresponding TCP specification was released by IETF (please refer to 3.1 Standards compliance).

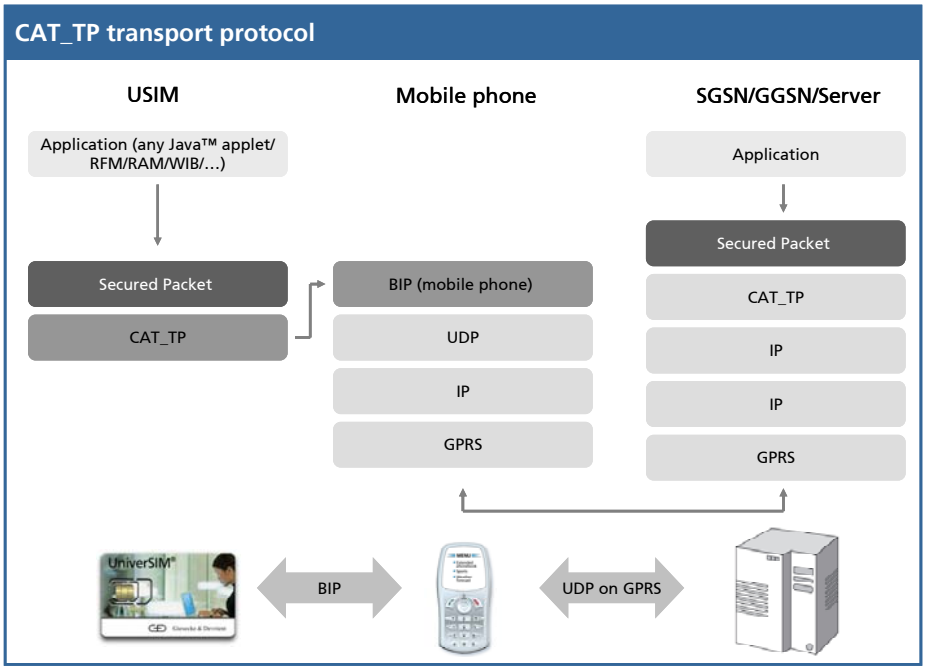
TCP runs on mobile phones whereas CAT_TP is implemented on a (U)SIM. For CAT_TP it means that all confirmations, time-outs and repetition counters have to be passed through the mobile phone ⇔ (U)SIM interface. This creates increased traffic through the I/O interface of the (U)SIM, and it is to be expected that the performance of CAT_TP is slower than with TCP.

TCP is a mature technology that has proven itself for decades on the Internet. Free, off-the-shelf server implementations are available for it.

The following diagrams describe the functional principles of and differences between the TCP and CAT_TP protocols, covering the aspects of (U)SIM, mobile phone and network.

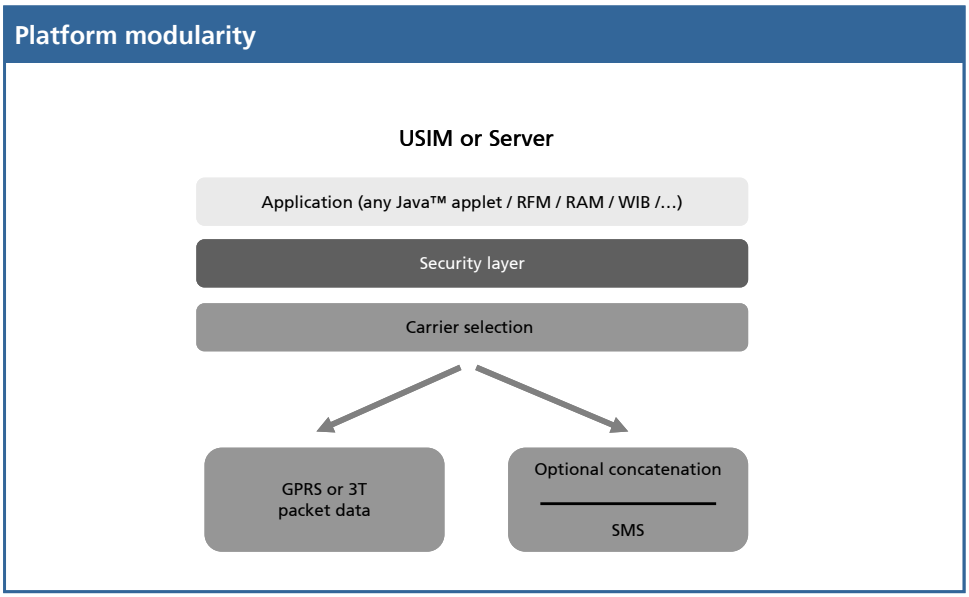
GPRS-based BIP system architecture





Platform modularity

The above mentioned solutions (TCP, CAT_TP) are allow applications to use different bearers for transferring data between the card and the server. The application and security layers can be the same on the card as well as on the server. Selection of the carrier and the carrier dependent adaptations (e.g. concatenation or reassembly for SMS) are performed below the security layer.



3.3 Data carriers

A typical solution will support one or all of the following data carriers:

- SMS will still be available for mobile phones not supporting BIP or if coverage for packet networks is not available
- GPRS in a GSM network. GPRS has the potential of providing up to 100 times the throughput of SMS
- 3G packet data bearer in a 3G network. A 3G packet network provides even higher data rates than GPRS

4 Terminal support

Today, terminal support for BIP enabled mobile phones is still limited. But with this technology becoming a mature market standard, we foresee all major mobile phone manufactures fully supporting this feature throughout their product portfolios in the near future. To ensure smooth migration towards BIP technology, both on mobile phones and (U)SIMs, G&D has teamed up with every major handset manufacturer for interoperability testing.

With respect to the different implementation possibilities, please refer to section 6 “Service development”.

5 Service request initialization

5.1 Application initiated service request

Depending on the application and the service, one solution supports the "pull" feature, since it is the user who has to initiate the communication flow. In such cases, the user triggers a service, via a SIM Application Toolkit menu implemented on the (U)SIM, for example. By browsing the menu and selecting one of the available options, he actively "pulls"' for further information, e.g., via GPRS or 3G.

For further information please also refer to section 6.3 "User information retrieval".

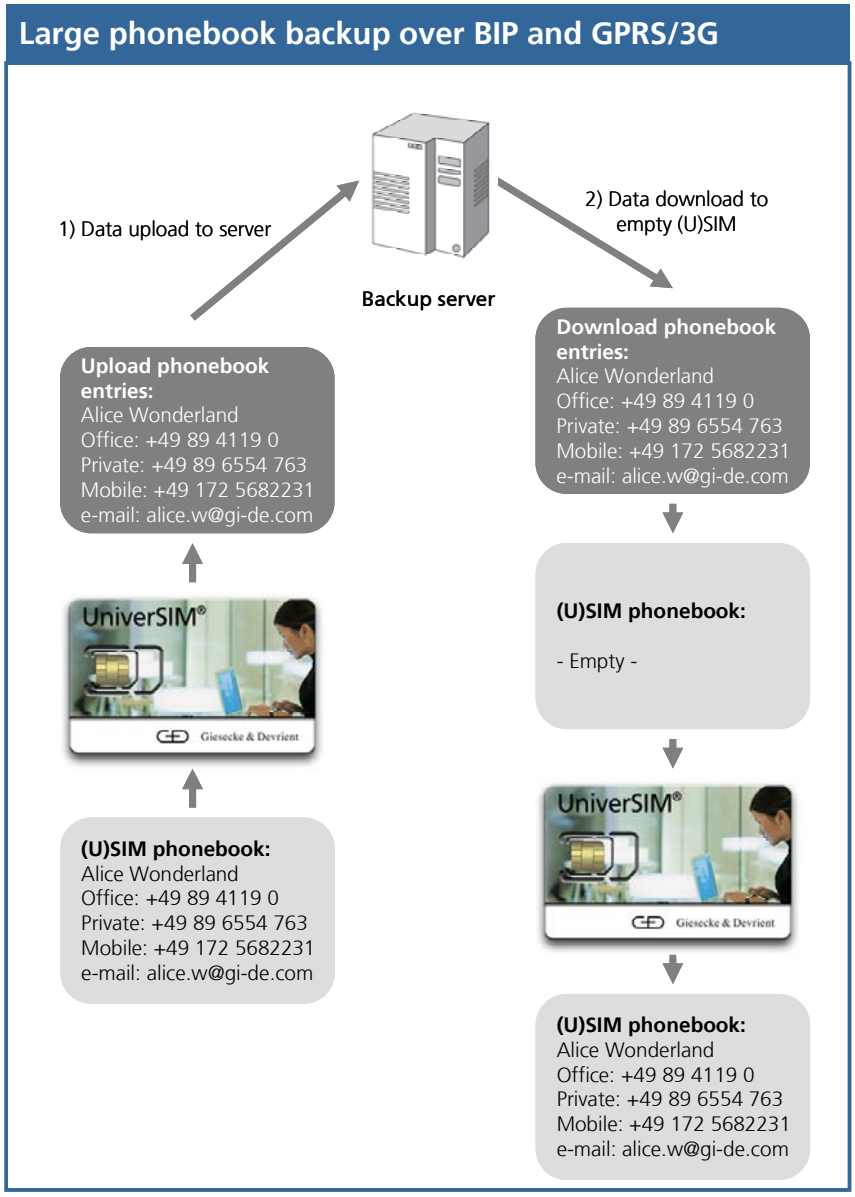
5.2 Server initiated service request

For services such as RAM and RFM (e.g. phonebook back-up) the application on the (U)SIM can be triggered by the network using a special "push" mechanism. This push mechanism (Push Short Message) is send to the card by the server in order to tell the (U)SIM application on the UICC to open the BIP communication channel (e.g. GPRS, 3G). As soon as a data channel has been established, an applet can be downloaded at a high data rate or the SIM phone book can be backed up on the server.

6 Service development

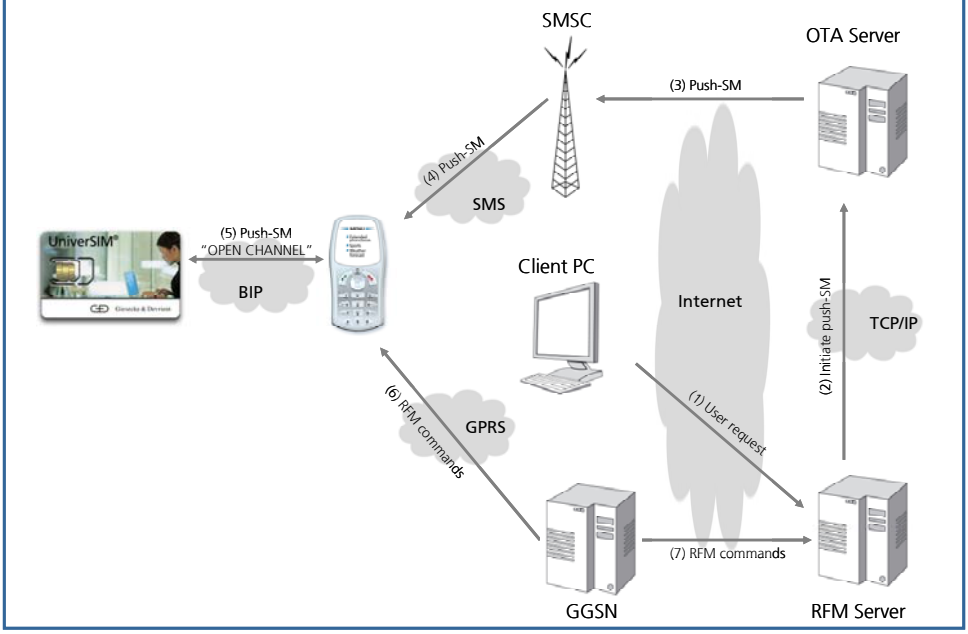
6.1 Application download and file management

Figure 3 illustrates phone book synchronization relying on GPRS or 3G as bearers. BIP/TCP is used for the transmission protocol. The high-speed protocol approach overcomes the limitations (e.g. speed) of today's commonly used technology for remote file or applet management (e.g. SMS).



In this scenario a user requests a phone book backup from his operator's customer service Web page. The request is issued from a client PC to a remote server, which is located on the network operator site. The server generates a Push SM and sends it, via the OTA server and the SMSC, to the (U)SIM card. The Push SM triggers the open channel command within the card and initiates upload of the phone book data—over GPRS or 3G—to the RFM server.

System architecture: Server initiated service request



Giesecke & Devrient

6.2 Description of a typical procedure

The TCP protocol supported by both a server and the mobile phone ensures data integrity between the two entities, via GPRS, for example. BIP commands allow the UICC to access the data through the GPRS channel.

The UICC initiates the opening of a GPRS channel. To achieve this, an OTA command, called a Push SM, is given. This command is pushed to the card by the server to tell the UICC application to open the GPRS channel. In addition, it is necessary to send the first IP packet including the mobile phone's dynamically assigned IP address to the server. An identification packet is defined for this purpose, containing some data the server uses to correlate the TCP connection with the Push SM that was sent to the card earlier.

Once the TCP connection is established, the server can send RFM data to the card. Subsequently, the card can send appropriate response packets back to the server.

After finishing the data exchange, the server may terminate the connection. In that case the mobile phone will issue the event "link-dropped" to the card. The second possibility is that the (U)SIM sends a CLOSE CHANNEL command to the mobile phone.

In the case of CAT_TP, the (U)SIM is responsible for the transport protocol instead of the mobile phone.

The table below illustrates the process of uploading a phone book:

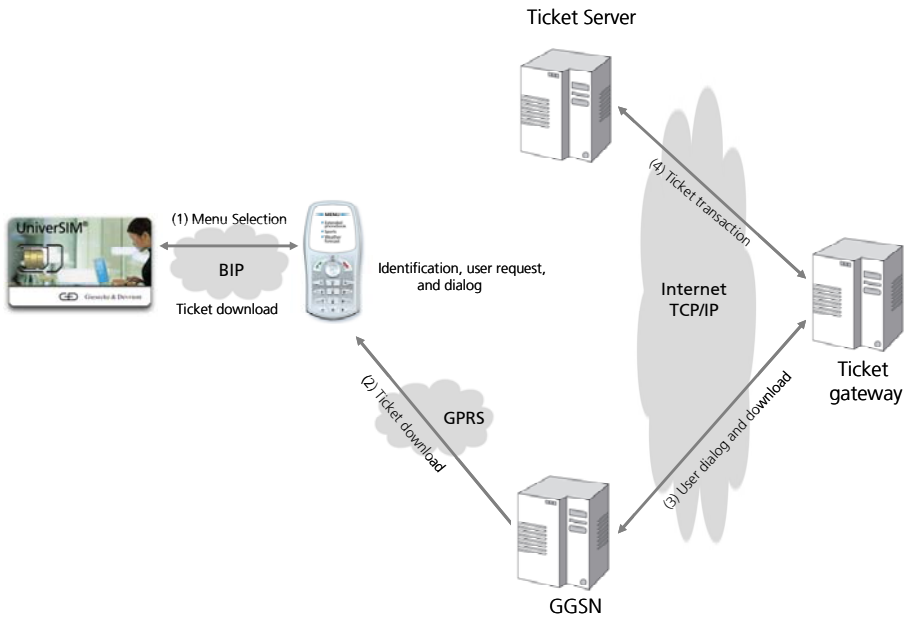
USIM	Mobile phone	Remote entity
		← PUSH SM request for BIP open and identification packet
	OPEN CHANNEL →	
		← RFM command data sent
	← DATA available event	
	RECEIVE DATA →	
	…	
	RECEIVE DATA →	
	Sent receipt acknowledge to server→	
	Process RFM commands	
	SEND DATA →	
	…	
	SEND DATA →	
		Send data →
		← RFM command data sent
	← DATA available event	
	RECEIVE DATA →	
	…	
	RECEIVE DATA →	
	Send receipt acknowledge to server→	
	Process RFM commands	
	SEND DATA →	
	…	
	SEND DATA →	
		Send data →
		← End session / terminate connection
	← EVENT link dropped	
	CLOSE CHANNEL →	

6.3 User information retrieval

G&D has developed an application, allowing users to access an information server via GPRS. This action is triggered by the user with a menu command via his or her mobile phone. After the application has opened the BIP/GPRS channel, the card sends an identifier to a server (gateway). The server responds by either sending further details for additional selection or the required information. This mechanism shows very good user acceptance, with an average system response time of 1 second or less.

In addition, the application might include a transaction protected end-to-end download of, e.g., tickets to the card via GPRS or 3G.

System architecture: Application initiated service request



7 Summary

With the availability of BIP supported infrastructure, the integration testing of cards and handset can begin, with initial commercial trials being realized in parallel.

As the (U)SIM is the property of the network operator and thus under his full control, BIP allows an efficient and highly effective administration of user applications, along with the intrinsic security aspects of the (U)SIM.

Most importantly BIP surpasses the conventional SMS approach by far. If only one out of several SMS is not received during the transmission of an applet, this means that the entire applet has to be resent by SMS. On the other hand, in a BIP session the transport protocol recognizes such transmission errors in real-time and requests only the missing data packet again.

G&D considers BIP technology to be a fast, reliable, and powerful tool for operators that allows card driven high-speed data services that rely on GPRS or 3G as bearers and BIP/TCP as the transmission protocol and that overcome the limitations of today's commonly used technology for remote operations (e.g. SMS).

8 Glossary

(U)SIM	Universal SIM
3G	The third generation of mobile phone technologies
BIP	Bearer Independent Protocol
CAT_TP	Card Application Toolkit Transport Protocol
GGSN	Gateway GPRS Service Node
GPRS	General Packet Radio System
IP	Internet Protocol
IrDA	Infrared Data Association
OTA	Over The Air
RAM	Remote Applet Management
RFM	Remote File Management
SGSN	Serving GPRS Service Node
SIM	Subscriber Identity Module
SMS	Short Message Service
SMSC	Short Message Service Centre
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UMTS	Universal Mobile Telephone System
WIB	Wireless Internet Browser

9 About Giesecke & Devrient

Giesecke & Devrient (G&D) is a globally operating technology group. Established in 1852, the company initially specialized in banknote and security printing, later adding automatic currency processing equipment to its product portfolio. Today, G&D is also a leading supplier of smart cards and cutting-edge system solutions in the fields of mobile communications, electronic payment technology, health care, identification, transportation, and IT security (PKI).

The G&D Group, based in Munich, Germany, comprises 52 subsidiaries and joint ventures in all parts of the world, employing almost 7,300 people, with around 3,800 of those outside Germany. In the 2004 business year, the group generated sales worth €1.16 billion.

As a leading manufacturer of (U)SIM cards for 2G and 3G networks, G&D provides operators with (U)SIM-based solutions for smooth migration from 2G to 3G, with OTA server solutions and service hosting as well as with logistics services. With its (U)SIM card products and services, G&D offers tailor-made packages from a single source: from (U)SIM lifecycle management to cost-effective (U)SIM ordering and production process to the complete development and deployment of mobile services.

G&D has a strong international orientation. Subsidiaries and joint ventures operate in Germany, Argentina, Australia, Bahrain, Belgium, Brazil, Canada, China, Egypt, Greece, Hong Kong, India, Italy, Japan, Korea, Luxembourg, Malaysia, Mexico, Morocco, Nigeria, Portugal, Russia, Singapore, Slovakia, South Korea, Spain, South Africa, Taiwan, Turkey, the UK, the USA, the United Arab Emirates, and West Africa.

Security and competence are the international high-tech group's core concepts. Its customer-focused products, systems, and services make G&D a reliable partner for any organization needing to solve complex problems in security-related fields.

For more information about the subject of this White Paper, please contact

telecom@gi-de.com

Giesecke & Devrient
GmbH
Prinzregentenstrasse 159
P.O. Box 80 07 29
81607 Munich
GERMANY

Phone:
+49 (0)89 41 19 - 15 43
Fax:
+49 (0)89 41 19 – 15 40

www.gi-de.com/telecom
telecom@gi-de.com