(i.e. security-enhanced) QUIPU-8.0 library functions for this DUA functionality. These library functions are not included in the SecuDE package, and a security-enhanced QUIPU-8.0 installation is additionally required (the security-enhanced Isode/QUIPU libraries libisode.a and libdsap.a are needed to be able to bind the application programs).

Alternative 3 requires a security-enhanced version of Quipu which can be obtained as a separate distribution from GMD.

The security-enhanced version of Quipu also contains software for a secured X.500 DSA. "Secured" means the ability to perform strong authentication during association setup between DUA and DSA, and subsequent signed operations at the DAP level. The DAP operations into which we have incorporated strong authentication are those assigned by the standard (X.511) for that purpose, i.e. Bind, Read, Compare, Search, List, AddEntry, RemoveEntry, ModifyEntry, and ModifyRDN. We have provided both SIGNED arguments and SIGNED results.

1.4 Use of Smartcards

SecuDE-4.1 supports the use of the GAO/GMD smartcard package Starcos 1.0 as one realization of the PSE. A serial line interface with 19.200 Baud is required to connect the Starcos terminal to the workstation. The Starcos terminal is a high-security crypto device which performs RSA and DES and provides a number of physical protection features. RSA key pairs are generated in the Starcos terminal. Secret RSA keys never leave the terminal.

2 A Brief Tutorial to Security

Since computers and computer communication are increasingly being used to store and exchange assets, measures have to be introduced to protect those assets against accidental or intentional loss, alteration and misuse. The assets to be protected can be of very different nature. They may consist of system resources owned by service providers who offer access to data bases, information systems or general computer services, they may comprise information which is stored and exchanged with the help of computers, and they may even comprise electronically signed and stored contracts by which other parties can be held responsible, or other electronically processed information which guarantees bindings of responsibilities or legal bindings in organizational contexts.

The latter examples show that new security techniques are not only needed in areas where classical security means as the usage of passwords have been proven to be unsufficient. Security is needed for areas where the application of computer communication is going to: as a means for cooperative work which may span over organizations between an open number of partners who may have conflicting interests and who possibly don't know each other when the communication starts. For this area, known as *open telecooperation*, advanced security techniques are a necessity.

Security is needed by both users of computer systems and providers of computer services. The classical way of achieving security reflects more to the interests of system providers

than to the interests of users. First, users are often rigidly restricted to services and system resources which they have paid for or which system administrators and service providers believe to be sufficient for the user's needs, second, access to system resources and information is provided by authentication techniques based on passwords which protect, in the best case, the system providers and the users among each other, but which do not protect users from privileged personnel, and third, the user's activities are often traced as comprehensively as it is necessary for the system administrator's needs. System providers and system users, however, have different interests. Central user identification, service restrictions and activity traces help the providers to protect their systems and to get their payment, but they limit the comfort of users and, more seriously, they jeopardize the privacy of users. This leads to closed systems. On the other hand, open systems which do not provide the possibility to users to set up closed subenvironments are unusable for a lot of applications. Open systems in which users are able to demand services, in the ideal case, spontaneously, unlimited, if desired anonymously, without prior registration and without succeeding system trace, cannot be realized by the conventional password oriented means.

2.1 Key Issues of Security

We can observe basicly four types of threats against communication security in open networks which can be qualified as follows:

- Unauthorized release of information by passive observation.
- Unauthorized modification of information, i.e. changing, duplicating or replaying exchanged information between two entities.
- Masquerading in various forms.
- Repudiation of communication, both by the originator or the recipient of communication information.

Authenticity is the key issue of security. Authenticity of the subjects (persons, organizational instances, program instances, hardware components) and of the objects (information, files, programs, keys) of information processing systems is the basis where the transferability of responsibilities relies upon, which in turn is the basis of every kind of cooperative work. Security requirements as integrity of data, access control, non repudiation or prevention of masquerade (i.e. playing the role of others) can only be served if one is able to rely on authentic partner relations.

Confidentiality is an issue, too, for a number of applications. This is the classical playground of cryptography. Information which belongs to the privacy of people like personal data, medical data etc., or information which represent an economic asset for individuals or organizations, should not be transmitted in cleartext over public networks if the disclosure of such information by unauthorized people could lead to economic or other damage. A new dimension of eavesdropping threats comes through the use of local area networks. Systems which are connected to the entry points of public data networks are rarely single computers which can be additionally protected by physical conditions. In most cases local

area networks or distributed systems are behind the wide area network. An Ethernet for instance is extremely easy to monitor if one has access to the coax cable, and the extensive use of distributed file systems like NFS leads to the situation that often one even doesn't know what heavy network activities are triggered by a command which looks like a local file access at the operating system interface. This example also shows that standard measures against eavesdropping as line encryption wouldn't help here. End-to-end encryption between the connected applications is essential in many cases, while encryption measures betwen network components are additional possibilities which might be useful to encounter traffic analysis and the like.

However, it should be noted that achieving confidentiality is not possible without authenticity. One must be sure with whom to exchange or share keys for confidentiality purposes, otherwise encryption might not be of great value. Authenticity is a prerequisite for other security services and therefore the key issue of security.

To summarize, we can observe a need for

- the possibility of authenticly identifying acting persons or instances in a decentralized and user controlled way which requires the disclosure of not more individual information than necessary in order to satisfy the legitimate interests of all concerned parties, and which avoids any unnecessary involvement and traces of central authorities,
- the possibility of providing and verifying a proof of authenticity and integrity of information,
- and the possibility of guaranteeing confidentiality and privacy in a multi-party environment.

2.2 Cryptography

The basic means to provide security of the nature mentioned above is cryptography. Cryptographic algorithms are being used for two purposes. One is to prove to others that one is in the possession of a certain key. If the partner or verifier is able to decrypt an information which was previously encrypted using this key, the proof is provided. If it is assured by other means, in addition, that no other person or instance can be in possession of this key, the use of this key produces a link to the user of the key. This is the way authentication is done. The other is to use cryptography in order to conceal information, i.e. to avoid unauthorized disclosure of information. This is the classical application of cryptography which aimes at achieving confidentiality.

We can distinguish two main categories of cryptographic algorithms. One category comprises the **symmetric** algorithms where encryption and corresponding decryption is performed using the same key, but inverse functions. The best known symmetric algorithm is the *Data Encryption Standard* (DES) invented 1977 by the American NBS (National Bureau of Standards, now NIST) and internationally standardized as DEA1 (Data Encryption Algorithm 1).

The second category comprises the **asymmetric** algorithms. This type of algorithms was invented by Diffie and Hellmann in 1976 and uses different keys for encryption and

corresponding decryption. The two keys are mathematically dependent from each other, but it is a requirement to the algorithm that one key can be computed from the other key at most in one direction, while the other direction must be computationally unfeasable. This property allows to make one key (the one which can be derived from the other) public while the other key must be kept secret and unbreakably linked to a person or instance. Therefore this type of algorithm is also called **public key** algorithm.

The class of asymmetric algorithms can be subdivided into the two categories **reversible** public key algorithms and **irreversible** public key algorithms. Reversible algorithms have also the property that applying the encryption function to a cleartext followed by applying the decryption function to the ciphertext results in the cleartext again and has the same effect as doing it in the reverse order, i. e. we have

$$d(e(cleartext, E), D) = e(d(cleartext, D), E) = cleartext$$

with	e: encryption function	E: encryption key
	d: decryption function	D: decryption key

This property allows to use a single algorithm and even a single key pair for both authentication/integrity and confidentiality puposes in that you use your own secret key to produce a digital signature which can be verified by everyone through your public key, and that another person uses your public key to send you information in a confidential way which you can decrypt using your secret key. The best knowm reversible asymmetric algorithm is the *RSA* algorithm invented by R. Rivest, A. Shamir and L. Adleman in 1978.

Irreversible asymmetric algorithms do not have this property, i.e it is not possible with them to recover the cleartext from the ciphertext, and they don't have encryption / decryption functions in that sense. With them it is possible to verify with a public key component that a digital signature was produced with the corresponding secret key component. Therefore this type of algorithm is also called **signature-only** algorithm. The best knowm signature-only algorithms are the *ElGamal* algorithm invented by T. Elgamal in 1985, and the NIST variant of this algorithm, the *DSA* algorithm, used for the proposed US FIPS *Digital Signature Standard* (DSS).

Symmetric algorithms can be realized very efficiently, but they have the problem of requiring a shared secret. Two partners using symmetric cryptography must have the *same* secret key. This makes symmetric algorithms unsuitable for proving individual identities to third parties because at least two share the same key and the knowledge of the key doesn't provide a link to an individual user. Another problem is the necessity to transmit symmetric keys accross networks if the communcating partners are on different places. Symmetric cryptography can be used for the purpose of authentication in conjunction with a central authentication server whom anyone trusts and who keeps the secrets of all partners.

The problem of the shared secret does not exist with asymmteric cryptography. Every person or instance, i.e. every subject, owns a unique *pair* of keys. One of them is to be published, while the access to the other must be unbreakably restricted to the subject itself through a secure local environment, e.g. a smartcard environment. By means of *digital signatures*, which are being generated through encrypting a hash value of the information to be signed using the secret key, and which can be verified by everyone through decrypting

the signature using the public key, authentic identifications and proofs of integrity can be exchanged in open systems. Confidentiality can be achieved, too, in the case of reversible algorithms (RSA) by encrypting the information with the recipient's public key. This can be done by everyone, but only the recipient is able to decrypt the information with his secret key.

The application of asymmetric cryptography leads to a number of practical problems, too. One of them is that most known asymmetric algorithms rely on complex mathematical problems of number theory and the usage of very large integer numbers, which makes them considerably slower than DES, for instance. Thus they are not suitable for the encryption of large amounts of data. A widely accepted solution is to encrypt data (for the purpose of confidentiality) using symmetric algorithms and to exchange the corresponding symmetric keys in encrypted form using reversible asymmetric algorithms.

2.3 Public Key Certification

Another fundamental problem, which arises in open environments with large numbers of partners who do not know each other, is the question of the authenticity of public keys. At the time of verifying a digital signature the verifier must be sure that the public key which he uses for the verification of the signature is the public key of the supposed signer, i.e. he needs a key-to-name binding which he can trust. Without additional measures each user would have to perform an out-of-band verification of the authenticity of each partner's public key before trusting it. The complexity of this problem can be reduced by *certifying* public keys through a third party whom both signer and verifier trust. This third party, the so called *certification authority* (CA), signs the user's public key and his name (plus some additional data like a period of validity) with its own secret key. This piece of data, signed by the certification authority, is called a *certificate*. The certificate can be verified with the public key of the certification authority. Now two partners can authenticate each other by first verifying the partner's digital signature with the partner's public key and then verifying the authenticity of the partner's public key through verifying the digital signature of the certificate using the public key of the certification authority. Only the public key of the certification authority must be trusted, thus reducing the number of public keys which the individual user has to trust to one.

In large user populations comprising perhaps millions of partners, a single certification authority is not sufficient. The public keys of certification authorities may be certified again by other certification authorities. One can imagine tree structures of certification authorities, or net structures in that CAs belonging to different trees cross-certify each other, thus providing certification pathes or chains of trust between individual partners.

2.3.1 Public Root Key

However, the chain of certificates cannot be endless, and the public key in the last certificate remains uncertified. This is called the *Public Root Key* which the user simply has to trust finally. The authenticity and integrity of this key has to be provided by out-of-band means. The key can be published, for instance, in a human readable form, and particular software may enable the user to compare this key with that what is stored in his computer.

Once the public root key has been entered into the local computer system, its integrity must be protected by local means (for instance through the use of smartcards). The public root key, though public, is as security sensitive as the personal secret key. They are the two ends of the security chain between two individual partners.

2.3.2 Certificate Revocation

A certification authority must be able to revoke a certificate which it issued prior to its expiration time. There may be many reasons for a certification authority to revoke a certificate:

- The user's secret key is assumed to be compromised whereby the corresponding public component is invalidated.
- The user's affiliation has changed whereby the distinguished name contained in the certificate's "subject" field is invalidated.
- The user is no longer to be certified by the CA.
- The CA's certificate is assumed to be compromised.
- The user has violated the CA's security policy.

A certification authority can mark a certificate which it issued as "invalid" by adding it to the list of revoked certificates.

Information relative to certificate revocation is propagated by means of revocation lists, so-called "black lists". Revocation lists must be made publicly available, for instance by being placed in the public X.500 Directory.

2.4 Key Management

Key management is the process of achieving suitable keys for the own use and making them available to the partners in a way that they are able to validate them and use them in the intended manner, and that nobody is able to misuse them. This means in the case of symmetric keys and asymmetric secret keys that they have to be transmitted confidentially (through encryption or out-of-band transport). In case of asymmetric public keys additional information (a certificate, for instance) must be available to the partner to be able to verify the authenticity of the key.

The same requirements apply for the communication between a certification authority and its user (which may be a certification authority again) for the purpose of public key certification. Keys must be exchanged between the CA and the user. There are basicly two alternatives for the operation of public key certification which have different security implications:

1. The CA generates the asymmetric key pair, certifies the public component, and provides the user the secret key, the certificate (which includes the public key) and possibly own certificates which link the whole thing to a common root key.

2. The user generates the asymmetric key pair and sends the public component to the CA. The CA certifies this, and provides the user the certificate and possibly own certificates which link the whole thing to a common root key.

In the first case there is a need for confidentiality-protected information exchange, in the latter not. Confidential transmission from the CA to the user is easy if a smartcard is being used which is generated at the CA site and physically delivered to the user. In case of transmission in electronic form a symmetric encryption key (or a password where a key can be derived from) has to be transmitted out-of-band. In the first case, the certification authority has control over the quality of the generated keys, in the latter case the user has complete control over his secret key. In both cases, however, an out-of-band information provision has to take place which gives the CA the required level of confidence in the user's identity and the name to be certified. Both types of CA – user interaction are supported by SecuDE.

2.5 Public Directories

The use of public key cryptography makes it necessary that one knows and trusts other's public keys. Public Directories like X.500 Directories may play a supporting role here. Users and certification authorities (if they are involved) have the following requirements when they use security services on the basis of public key cryptography:

- Users have the requirement to make their certificates publicly available and to have access to certificates of others and revocation lists in order to find out whether a certificate in question is still valid or has been revoked.
- Certification authorities have the requirement to make their certificates and revocation lists publicly available to a distributed community.
- Certification authorities have the requirement to exchange cross certificates with other certification authorities and make them publicly available.

Therefore the integration of public Directories (in particular X.500 Directories) into the security infrastructure is a vital part of SecuDE.

A public Directory appears not only as information provider as part of the public security infrastructure, but also as user of security services in order to protect its stored information from unauthorized access and to protect its communication. Security policies in case of the globally distributed X.500 Directory must aim at three major goals:

1. Protect the information base of the Directory.
2. Protect the internal and external communication of the Directory via DAP and DSP.
3. Protect the resources of the Directory.

These needs were the motivation for the development of the *Authentication Framework* (X.509) as part of the X.500 Directory standard where *strong authentication* methods on the basis of digital signatures and certified key-to-name bindings are being applied in

order to protect the X.500 Directory. The certification procedures and formats of X.509 are applicable in any context where public key cryptography is used. They play a central role in SecuDE. X.509 certificate formats have been adopted, for instance, in the Internet PEM environment.

2.6 Examples

Following are a few examples where digital signatures on the basis of asymmetric cryptography and confidentiality services on the basis of both symmetric and asymmetric cryptography are essential:

- *Electronic mail* is a very obvious example. The security of electronic mail must not be weaker than that of paper bound mail, i.e. it should be possible to sign mail and to transmit it confidentially. There are basicly two possible solutions to enhance electronic mail services with security features:

  One is to add security information to message bodies without affecting the functionality and protocols of the message transfer systems involved. The Internet RFCs 1421 - 1424, 'Privacy Enhancement for Electronic Mail' (PEM), provide such methods and coding formats for message encryption and authentication. Key certification is done here using ASN.1-encoded X.509 cerificates.

  The other solution is a full integration of security services into X.400 message handling systems which includes also the secure interworking of components of the message transfer system. CCITT Recommendations X.400 (1988) / ISO 10021 (Motis) contain a comprehensive treatment of security issues including security specific protocol elements. Key certification is again done by referring to X.509.

- *Public directories* which store and provide public information of users to support electronic communication between them have two important security aspects: First, they have to provide security related public information like certificates and black lists. In this role Directories are part of the security infrastructure. Second, they have to control the access to the Directory Information Base (DIB). Only authorized persons should be able to modify directory entries, and read access to directory data may be limited to certain persons. In this position Directories are users of security services.

  The CCITT Recommendations X.500 (1988) / ISO 9594 about directories basicly provide two methods of protecting the DIB with the help of digital signatures:

  1. *Strong Authentication* of the involved components during their association establishment (DUA-to-DSA and DSA-to-DSA).
  2. *Signed Directory Operations* when accessing the DIB.

  The *Authentication Framework* X.509 / ISO 9594-8 provides the basic procedures and formats for the application of public key based digital signatures. The certification techniques defined there are widely applicable outside the scope of directories, too.

- For *document exchange* on the basis of ODA/ODIF security services are required, too. Similarly to electronic mail, it must be possible to sign or conceal whole documents or parts of them, so that sender and receiver of documents can trust the