CRYPTONET: SECURE E–MAIL SYSTEM

Sead Muftic and Gernot Schmölzer
Department of Computer and System Sciences, Royal Institute of Technology, Stockholm, Sweden

Keywords: Secure E-mail, cryptography, SMIME, security architecture, SAML, smart cards.

Abstract: The paper describes new, innovative and highly secure E–mail system. The system, first, provides both standard security services for E-mail letters: signed and encrypted E–mail. In addition, address book is encrypted, thus E-mail addresses can not be stolen for spamming. Each E–mail server is protected using SAML authorization policy, so E–mails are received only from authorized senders. Finally, all E–mail addresses are validated and certified by specially designed Secure E–mail Infrastructure (SEI) Authorities, organized in a federated hierarchy. Thus CryptoNet Secure E–mail system completely eliminates spam, distribution of viruses, worms, and malware, and eliminates the possibility to use fake E–mail addresses.

1 INTRODUCTION

E–mail is one of the most popular Internet applications. Not only that it transfers E–mail letters, but it is also used to transfer binary (multimedia) attachments, various notifications, business documents, etc. These aspects make E–mail system even more important than its original purpose.

In terms of problems, they are numerous. E–mail today is overloaded with spam, which is one of the most serious problems today in the Internet. Another problem is that E–mail is today the main mean to distribute viruses, worms, malware, spyware and other forms of troublesome software. Finally, E–mail is also used to perform financial fraud, identity theft, intellectual property theft, and other serious Internet problems.

In terms of new opportunities, E–mail system can be used as a secure and reliable application for serious business transactions. For that, current E–mail systems must provide reliable and verifiable identities, secure and protected E–mail letters, and new services, like notifications of receipts, registered E–mail, authorizations, secure distribution of E–mails in groups, etc.

Based on all of the above, it is of high importance and high interest today to design, standardize and put in experimental operation a new, secure and reliable E–mail system. The system should eliminate all problems and issues with current E–mail implementations and at the same time fulfill some or all of the advanced user requirements. At the same time, the system should be suitable for transparent incorporation into the current E–mail components, infrastructure and protocols, so that it can be easily installed, deployed, activated and used on a large scale.

This paper describes the design, implementation and use of such secure, trusted, authorized, and reliable E–mail system, here called *Secure E–Mail* (SEM) *System.*

2 PROBLEMS AND REQUIREMENTS

New features of the SEM System can be structured in two groups: those solving *current problems* and the others, providing *additional features* and satisfying *additional requirements*. This section lists and briefly describes both of these categories and as such, it servers as description of features and properties of the new, SEM System, described in the subsequent sections of this paper.

2.1 Problems with Current E-Mail

Today, *authentication of users* from Mail Clients to Mail Servers is usually performed using username and password. This is generally considered as very weak authentication method and also as the source of many system penetrations.

The second problem is *protection of mailboxes* and *E–mail letters* on E–Mail Servers against illegal

Muftic S. and Schmölzer G. (2008).
CRYPTONET: SECURE E–MAIL SYSTEM.
In *Proceedings of the International Conference on Security and Cryptography*, pages 84-91
DOI: 10.5220/0001929800840091

and unauthorized reading. Today it depends on security features of native operating systems, which is either inadequate or most of the time even not enforced. The same is the case with client machines.

The third problem is *protection of E–mail letters* against illegal reading and/or modifications while in transfer. The interpretation of this aspect is that the intended recipient of an E–mail letter cannot be guaranteed to the sender and the original content of E–mail letters cannot be guaranteed to the recipients.

The next problem is *spam*. The essence of this problem is that mail today is delivered without authorization – in principle every sender and mail server may send an E–mail letter to any recipient.

Another problem is that content of the address book at the mail client (user workstations) is kept *in clear*. That is very often the source of stolen E–mail addresses, collected by spyware or viruses installed at client computers.

If users are using security features of the current E–mail clients, i.e. encryption and digital signatures, then corporate E–mails cannot be retrieved by *corporate authorities* and *law enforcement authorities*. This may cause problems in case of lost mail, terminated employees, and/or law enforcement procedures.

Finally, E–mail is used for *distribution of malicious* and *dangerous content*, like viruses, worms, spyware, bots, etc.

2.2 Requirements for New Services

In addition to the problems listed in the previous section, in order to be used for serious business transactions, E–mail system must support a number of additional requirements and desirable properties. Some of them are the following:

Handling of attachments is very inefficient. Today, if an E–mail letter with a large attachment is sent to a group of people, the large E–mail travels through many mail servers and reaches all recipients. Therefore, it overloads the network, mail servers' storage space and mail client's disk space. The attachments cannot be distributed selectively and efficiently.

Confirmation of delivery and *confirmation of receipt* are not supported today by most of mail clients.

Handling of certificates is, first, optional and second usually performed by the associated browser (Internet Explorer for the Outlook and Firefox for Thunderbird). Some E–mail clients cannot even handle and use certificates. *Verification of certificates* is also either optional or not available.

Usage of *smart cards* with current E–mail systems is very complicated and therefore very rarely used.

Authorization, for users to submit E–mail to the mail server and to send E–mail to the designated recipient and for mail servers to submit mail to the designated mail server, is not enforced. This is the main reason for spam, since any mail server can send E–mail to any other mail server.

There are no *cross–domain* bilateral or multilateral arrangements, synchronization of policies, coordination of assurance levels, negotiation of security and cryptographic protocols and algorithms, etc., all features already standardized for Web services and many other types of network applications.

3 LAYERED ARCHITECTURE OF THE SECURE E–MAIL SYSTEM

SEM System is created through *(a)* new E–mail client, *(b)* security extensions of E–mail servers, and *(c)* additional infrastructure components. If deployment is based on usage of current clients, then only a limited set of security problems and requirements from section 2 can be addressed.

The concept of the SEM System is a layered architecture, comprising four layers. The layering principle is that components at the higher layer "sponsor" components at the lower layer. The bottom layer is SEM Clients layer. The next layer is SEM Servers layer. The layer above is Credentials Servers layer. It contains CA Servers and SoA Authorization Servers (usually called Policy Decision Points – PDP). The components located in these three layers are deployed inside an organization i.e. inside an administrative or security domain. The fourth layer is new, here introduced as *Secure Mail Infrastructure (SMI),* comprising SMI Servers. Their functions, topology and inter–relationships are described in section 7 of this paper.

4 LAYER 1: SECURE E–MAIL CLIENTS

SEM Client performs the following functions and supports the following standard mailing and additional security features:

4.1 Standard Mailing Functions

SEM Client performs all standard mailing functions: reading and sending E–mail letters, displaying and deleting retrieved E–mail letters and attachments, handling of local mailboxes, editing/using local address book, simple configuration of the client, spell–checking, etc.

4.2 Handling of Certificates

The first security extension of the SEM Client is handling of certificates. It is performed in the following way:

- Two self–signed certificates (digital signature and key exchange certificates) are automatically generated upon initial startup of the Client.
- If smart cards are installed, keys are generated in the card and certificates are stored in the card. The card is used to perform SEM Client's security functions.
- If CA Server is configured, two certificates are requested and received from the CA Server.
- If PKI policy requires, key exchange key pair is generated and escrowed by the CA Server.

4.3 Standard Security Services

With possession of the two certificates, SEM Client performs standard security services for E–mail letters: digital signing E–mail letters and encryption/enveloping of E–mail letters. In order to perform these two functions, SEM Client has the following capabilities:

- It can inquire and obtain recipient's certificate by sending request to its own SEM Server (see also section 5.1), which re–directs the request to the recipient's SEM Server, which returns the certificate to the sender's SEM Server, which passes it back to the sender's SEM Client.
- If the intended recipient does posses the certificate (this is always the case of SEM System users), all E–mail letters between two users are encrypted and signed.
- If the certificate request does not return recipient's certificate, all E–mails to that recipient are signed, but not encrypted.
- Certificate chain is included in an initial E–mail to the SEM System user (recipient).
- All received certificates are verified before stored in the local certificates database.

4.4 Usage of Smart Cards

If smart cards are available, SEM Client uses smart cards. Smart cards are used in the following way:

- Key pairs are generated in the card and certificates are stored in the card.
- All security functions (digital signatures and enveloping of the E–mail letter encryption key) are performed by the smart card.
- Smart card is also used to store encryption key for the Address Book.

4.5 Protection of the Address Book

All entries in the Address Book are kept encrypted. The entries are decrypted on the fly when listed on the GUI panel of the SEM Client. Cryptographic protection of the Address Book is performed in the following way:

- Cryptographic key (symmetric) is generated at the initial activation of the SEM Client.
- The SEM Client has the function to change address book encryption key, in which case address book must be re–encrypted.
- If smart cards are used, the key is generated and kept in the card. In case that the card is lost, the key is escrowed at the SEM Server.
- If the card is not used, the key is stored in the SEM Client's local file, encrypted with user's login password. The key is decrypted when SEM Client is started, so address book key and login password are not available in clear in the system during its operations.
- If the new entry in the Address Book is created or an existing entry is updated, the SEM Client decrypts the Address Book's key, creates new entry or updates the existing entry.
- The entries in the Address Book have sequence numbers, so they are displayed in clear, but they do not have to be decrypted on the disk if an entry needs to be deleted.
- If the address book encryption key is stored in smart card and the card is lost or if the local key file is corrupted, then the Address Book can not be recovered, so encryption key is escrowed/enveloped at the SEM Server.
- SEM Client has the function to fetch Address Book's encryption key from the SEM Server, if the recovery is needed.

4.6 Confirmations

SEM Client provides three confirmations to the sender for each E–mail: *confirmation of delivery*,

confirmation of receipt, and *confirmation of acceptance*. SEM Client performs the following functions with confirmations:

- Receive confirmation of delivery from the recipient's SEM Server.
- Receive confirmation of receipt from the recipient's SEM Server.
- Receive confirmation of acceptance from the recipient's SEM Server.
- Maintain the status of E–mail letters in the Outbox, based on those confirmations, and display that status when listing the Outbox.

4.7 Strong Authentication with the SEM Server

Since both, SEM Client and SEM Server have their key exchange certificates, these certificates are used to perform strong authentication between the SEM Client and SEM Server. The transfer protocol is SSL, so that all transfers of E–mail letters between SEM Client and SEM Server are strongly protected.

4.8 Management of Authorizations

Distribution of spam is eliminated by applying the standard concept of authorizations adapted from the service–oriented architecture (SoA) to the SEM System. Sending of an E–mail letter is an action performed by the sender's E–Mail Server (in SoA terminology – *service consumer*) using recipient's E–Mail Server (*service provider*). This action must be authorized. Using the concept of role–based access control and XACML policies, authorizations are based on "white lists", applied by SEM Servers at both ends of the transmission – by senders' SEM Server and also by receivers' SEM Server:

- At the receiving SEM Server the white list includes all users and/or mail domains from which the SEM Server accepts E–mails.
- At the sending SEM Server the white list includes all users and/or mail domains to which the SEM Server is authorized to send E–mail.
- White lists at the SEM Server are maintained both, by security (mail) administrators and also by users: administrators register mail domains, while users register individual mail addresses.
- Since mail addresses in the incoming mail to the SEM Server may be forged, they are digitally signed by the SEM Authorities.
- This solution does not prevent spam from reaching receiving SEM Servers, but such E–mails will be rejected by those Servers, while between members in the SEM System spam is completely eliminated.
- The more standard mail servers are enhanced with add–on SEM Servers, spam mail can be eliminated already at the sending SEM Servers. Thus, spam mail in the overall Internet can be greatly reduced.

4.9 Synthesis of SEM Client Security Functions

Security features of the new SEM Client, described in this section are shown in Figure 1. E–mail letters are protected (signed and enveloped), both in transfer and in mailboxes. Address book entries are encrypted. Attachments are signed and enveloped, and efficiently distributed using pull method.

Not shown are security functions related to Credentials Servers located at the Layer 3 of the SEM System architecture and SMI Servers, located at the Layer 4 of the SEM System architecture. They are shown in Figure 2 (section 6) and in Figure 3 (section 7).

5 LAYER 2: SECURE E–MAIL SERVERS

SEM Servers provide security extensions for standard mail servers. They are implemented as an add–on component to the standard mail servers (Figure 1). It may be noticed that SEM Servers are located between standard mail servers and the Internet and in that sense they represent some form of "E–mail gateways".

Handling authorizations at SEM Servers by SEM Clients is not shown. It is shown in combination with Policy Servers, located at the Layer 3 of the SMI architecture.

5.1 Handling of Certificates

Each SEM Server has its own two certificates: digital signature and key exchange certificate. Therefore, the Server performs the following functions with certificates:

- At the initial start–up, generates two self–signed certificates if CA Server is not configured, otherwise requests two certificates from the CA Server.
- Receives and stores client's key encryption certificate.

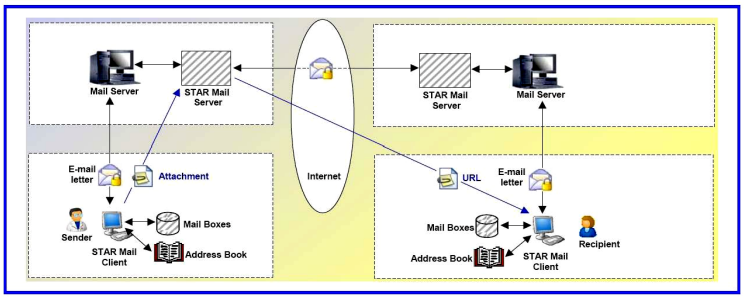

Figure 1: Security Features of SEM Clients and SEM Servers.

- Receives requests from local SEM Clients for key exchange certificates of their partners (mail recipients).
- Sends certificate requests to recipient's SEM Server, receives recipient's key exchange certificate, and returns it to the SEM Client.
- Receives certificate requests for key exchange certificates of local SEM Clients from remote SEM Servers, and returns those certificates.
- Requests and receives recipient's SEM Server URL from the SMI Server.

5.2 Address Book Encryption Keys

SEM Servers store enveloped encryption keys for address books of local users. To assist users with handling of address books keys, SEM Server performs the following two functions:

- Receives and stores user's address book encryption key.
- Sends address book encryption key to the user.

5.3 Confirmations

SEM Server sends the following two types of confirmations to the sender:

- Confirmation of delivery, when an E–mail letter is received from the remote SEM Client.
- Confirmation of receipt, when an E–mail letter is sent to the local SEM Client (receiver).

5.4 Handling of Attachments

SEM System uses pull method to handle distribution of attachments. SEM Server performs the following functions in order to handle the attachments:

- Receives attachments from local SEM Clients and stores them locally.
- Distributes attachments, when requested by recipient's SEM Clients.
- Manages Attachments Table, as described in section 5.8.

5.5 Enforcement of Authorizations

SEM Servers maintain white lists for both, incoming and also outgoing E–mail addresses. These lists have two types of entries: E–mail domain entries and individual E–mail accounts entries. Domain entries are specified in the *Domains Policy* document, created by Security Managers at SAML Policy Servers. Individual E–mail account entries are specified by users in *Accounts Policy* files at SEM Servers. In order to support enforcement of policies for sending and receiving E–mails, SEM Server performs the following functions:

- Receives Domain Policy file from SAML Policy Server.
- Creates and updates Account Policy file by local users.
- Enforces authorization policy for outgoing mails by verifying E–mail addresses of outgoing E–mails and making decisions to send them or reject submission.
- Enforces authorization policy for incoming mails by verifying E–mail addresses of incoming E–mails and making decisions to receive them or reject receipt.

5.6 Cooperation with SMI Servers

For cooperation between SEM Servers and SMI Servers, see also section 7.2.2. SEM Servers can request validation of their domain E–mail addresses, receive, and also store their validated addresses.

6 LAYER 3: CREDENTIAL SERVERS

At this layer there are two types of servers: PKI Certificate Authority (CA) Issuing Server and SAML Policy Server (Figure 2). In principle, there should be one of each of those two servers per mail domain, but multiple servers may also be used.

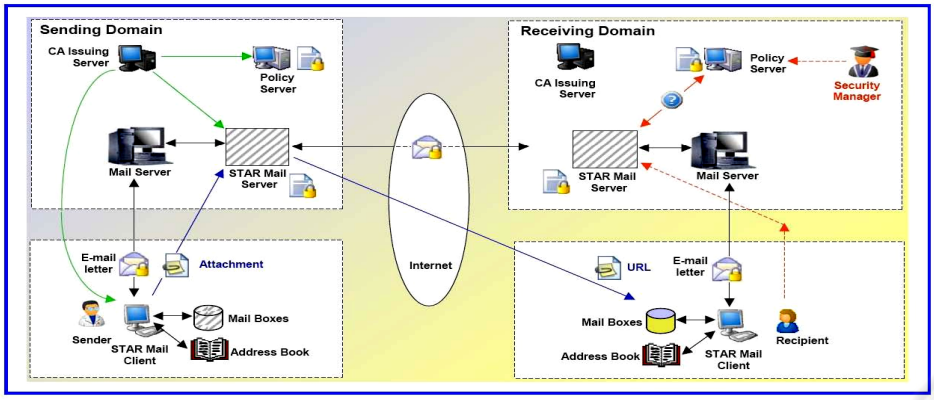

Figure 2: Credentials Servers: Issuing PKI Server and SAML Policy Server.

Both of these two servers are connected to their corresponding servers in the PKI and SMI (Layer 4 of the security architecture). CA Issuing Server is connected to the PKI Policy Server and through it to the Top (Trusted, Root) Server. SAML Policy Server is connected to the SMI Server.

6.1 CA Issuing Server

This is standard Certificate Authority Server, issuing and distributing X.509 certificates. It issues certificate to all entities in the SEM System: users, SEM Servers, and local SAML Policy Server.

6.2 SAML Policy Server

This is standard SAML Policy Server, which functions as Policy Decision Point (PDP). It supports:

- creation of SAML policies and policy sets;
- distribution of policies to SEM Servers, which are Policy Enforcement Points (PEP), so that authorization decisions are made locally by the SEM Server;
- making decisions based on SAMLAuthorizationRequests received from SEM Servers and returning SAMLAuthorizationResponses.

Standard SAML policies are role–based. Users and roles are registered and roles are assigned to all active entities. Then authorization rules are created as combination of roles, actions and decisions. In case of the SEM System actions are *send* and *receive* mail and SEM Servers are treated as users in the policy enforcement system. In order to use standard format of the XML policies, in the SEM System there is only one role: mail server. Thus, particular mail server (mail.localServer.com) is specified as the *user*, the *role* is mail server, and *actions* are *send* and *receive* E–mail letters. *Decisions* are standard SAML PDP decisions: *permit* or *deny*.

In the SEM System applications are remote SEM Servers to which E–mail letters are being sent or from which E–mail letters are received. The structure of the rule in the SEM System is:

Role	Application	Action	Decision
`mail server`	`mal.remoteServer.com`	`send`	`permit`
`mail server`	`mail.remoteServer.com`	`receive`	`permit`

The interpretation of the first rule is that all active entities that have the role *mail server* are permitted to perform specified action (send E–mail letters) with the specified application – remote SEM Server. The second rule indicates that all active entities that have the role *mail server* are permitted to perform specified action (receive E–mail letters) with the specified application – remote SEM Server. These two rules indicate that the local SEM Server may exchange E–mails with the remote SEM Server.

Since in the local policy there is only one active entity – SEM Server with the role *mail server*, the rules in the table above regulate exchange of E–mail letters of the local SEM Server with the remote SEM Server.

7 LAYER 4: PKI AND SMI SERVERS

In order to connect and synchronize security policies and functions across multiple domains, a security infrastructure is needed. For use of certificates across multiple domains, PKI is needed. In order to synchronize secure E–mail functions across domains, new infrastructure, in this paper called *Secure Mail Infrastructure* (SMI) is needed.

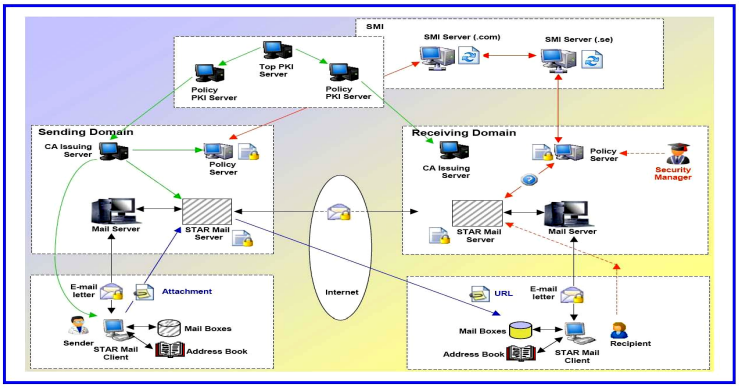

Figure 3: PKI and SMI – Servers and Protocols.

In order to provide their specific services to local domains, both infrastructures comprise specialized servers and protocols between them (Figure 3).

7.1 PKI Servers

PKI comprises two types of Servers. At the top of the Infrastructure is the Top (Trusted) Server. Its certificate is self–signed and requires special off-line protocol in order to be transferred to the lower level entities, verified and adopted by them.

Below the Top CA Server are Policy CA Servers. They enforce different PKI policies and impose those policies to the lower level servers – CA Issuing Servers.

7.2 SMI Servers

SMI Servers are needed for two purposes: validation of E–mail addresses and federation of SEM Servers located in individual mail domains.

7.2.1 Validation of E–Mail Addresses

With all the components, functions and their security features up to and including Layer 3, it is still possible to send spam to remote SEM Servers. The reason is that **From:** field in the E–mail letters may easily be faked. Such E–mails would be accepted by SEM Servers, since hackers would send spam E–mails with From: addresses of legitimate E–mail users, especially those in the white lists of the SEM Servers. In order to prevent that, there must be a mechanism to verify that all E–mail addresses used in the SEM System are original. This means that the E–mail address of each user must be certified (signed) by an authority and E–mail address of the domain must also be certified. The authority to certify E–mail addresses of users is Security Manager in the local domain. For the domain E–mail address, external certification is needed. Otherwise, all E–mail addresses in a domain would be self–certified and therefore not trusted and verifiable.

One function of SMI Servers is to validate and certify the E–mail addresses of the mail servers – domains. This effectively represents *registration* of a domain in the SMI. Such validated E–mail entries are returned to the SEM Server and used for construction of E–mail accounts for users.

7.2.2 Federation of SEM Servers

When an SMI Server validates the domain E–mail address of one of the SEM Servers, as the result of that process it also saves URL of the SEM Server. When SEM Client inquires key exchange certificate of one of its partners (recipients), it contacts its own local SEM Server. In order to fetch the certificate and deliver it to the local client, SEM Server must know URL of the recipient's SEM Server.

SEM Server will obtain that address from the SMI Server. SEM Servers are capable to request E–mail address validation from SMI Servers and obtain validated E–mail address.

8 COMMENTS AND CONCLUSIONS

8.1 Problems and Requirements

It may be easily verified that the proposed system, in its full scope, with all its components and functions, can eliminate all problems and fulfill all requirements listed in section 2.

Users are authenticated using their certificates, so user passwords are not needed at Mail Servers.

E–mail letters are fully protected, both in transfer and when stored in users' or mail server's mailboxes. Spam is largely eliminated. Theft of E–mail addresses from address books is eliminated. Corporate and law enforcement authorities can reliably use the System. Distribution of malicious content is greatly eliminated. It can be received only from trusted users, but this threat can be eliminated by extending SEM Servers with virus detection filters.

The system also provides all additional features and properties listed in section 2.2. It handles attachments very efficiently, since they do not float to all recipients, whether they need them or not. The system provides to senders three types of confirmations, so it can be used for exchange of serious business documents.

8.2 Gradual Deployment

The SEM System can be gradually deployed. As the first step, users may use only SEM Clients, without SEM Servers and Credentials Servers. In that case they can perform all standard E–mail functions and they can use security services available with existing E–mail clients: signed and encrypted E–mail.

In the second step, SEM Servers are installed. User security functions are now extended with additional security services of the SEM System, like exchange of certificates with their partners and efficient distribution of attachments.

As the third step, Policy and PKI Servers are installed. Now, users' certificates may be validated within the domain and authorizations are enforced.

Finally, if CA Issuing Server and SEM Server are linked to the SMI Servers, then the full scaling of SEM System across Internet is possible.

8.3 Applicability to Web–based E–mail

This paper describes E–mail system which is based on the use of full E–mail clients ("thick client"). The system is equally applicable to the Web–based mail ("thin client"). All features of SEM Clients can be made available using standard browsers. Since SEM Servers are extensions of mail servers, they can serve the same purpose with Web Servers acting as mail servers.

8.4 Increasing Assurance Levels

The system also supports the approach with increasing level of assurance. Lower assurance is the case when all cryptographic and certificate functions are performed in software and when certificates cannot be globally validated. Increased levels of assurance is use of PKI for the full validation of certificates and use of smart cards for storage of cryptographic parameters and execution of cryptographic operations

The most important is that even at the lowest level of assurance, all E–mail letters are strongly protected, spam is greatly reduced and distribution of malware is completely eliminated