



Service Definition

TABLE OF CONTENTS

1	INTRODUCTION	3
2	SERVICE DESCRIPTION	3
2.1	How Protectoria Works	3
2.1.1	Trust Levels	5
2.1.2	Sending Protected Messages	5
2.2	Account Types	6
2.2.1	Standalone	6
2.2.2	Integrated	6
2.2.3	Account administration	7
3	GETTING CONNECTED	7
3.1	Registration	7
3.2	Payment and Account Credit	7
3.2.1	Pay-as-you-go	7
3.2.2	Pay-per-user	7
3.3	Account Administration	8
4	PRICING	8
4.1	Charges	8
4.2	Currency	8
4.3	Account Credit Validity	8
4.4	Mailbox Size	8
5	SECURITY	9
5.1	Standards and Protocols Employed	9
5.2	Personnel	9
5.3	Threat Protection	9
5.4	Login to Webmail	9
5.5	Configuration Limitations	9
5.6	Procedures	10
5.7	Customer's Own Security Measures	10
6	CUSTOMER SERVICE	10
6.1	Contact Options and Response Times	10
6.2	Authorized Contacts	10
7	TECHNICAL SPECIFICATION	11
7.1	Operational Environment	11
7.1.1	Physical Access Control & Personnel	11
7.1.2	Power & Cabling	11
7.1.3	Maintenance	11
7.1.4	Monitoring	11
7.1.5	Disposal and Reuse of Media	11
7.1.6	Backup and Restore	12
7.2	Maintenance Window	12
7.3	Prerequisites and supported software	12
7.3.1	Basic User Prerequisites	12
7.3.2	Technical Prerequisites and Supported Software	12
7.3.3	Protectoria Certificate Requirements	13
8	CONTRACTUAL FRAMEWORK	13

1 INTRODUCTION

Protectoria® is a messaging service delivered by Message Management AS. The service enables customers to send protected e-mail messages to any recipient possessing an e-mail address, mobile phone and access to the Internet. Protectoria ensures that access to the message is authenticated and communication from sender to recipient is encrypted. Customers of the service can either use Protectoria Webmail supplied by Protectoria or one of the e-mail programs supported by Protectoria to send protected messages.

2 SERVICE DESCRIPTION

Protectoria is suitable to companies of all sizes as well as to individuals who have the need to protect their e-mail messages. This section explains how Protectoria works, the features available and the options you have for accessing the service.

2.1 How Protectoria Works

The following figures give a simplistic overview over how the service works. The figure 1 and 2 illustrates how Registered Protected messaging works. Figure 1 illustrates how Protected messaging works.



Figure 1

PROTECTORIA SERVICE DEFINITION

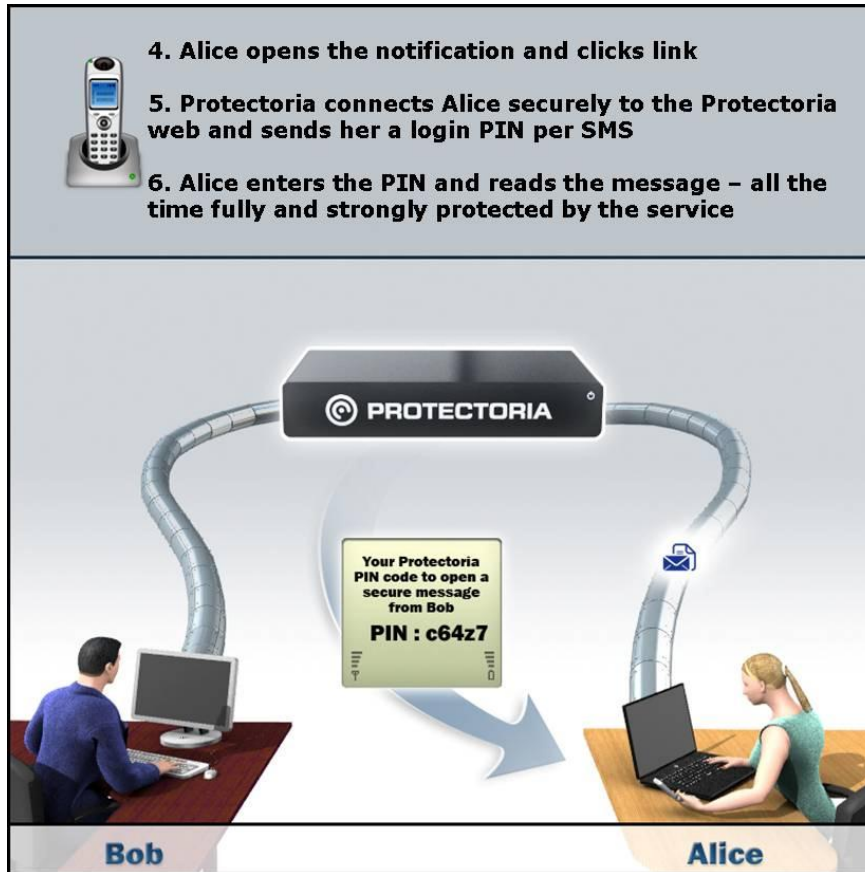


Figure 2

Protectoria supports also message relay between customer and customer partner email servers connected to Protectoria as illustrated below. In this user scenario emails are delivered to the recipients normal email Inbox without the necessity of authenticate with a PIN code. The sending customer decides if this option of secure email messaging shall be used.



Figure 3

PROTECTORIA SERVICE DEFINITION

2.1.1 Trust Levels

When you create protected messages, Protectoria will evaluate the recipient information that you enter as well as the options you have selected for the message. With this information, it will determine the trust level for your recipients and make a decision as to what security level is required for each of the recipients. As shown above, some recipients will by default be required to enter a PIN-code sent to their mobile phone to open the message, others not. As a sender, you always have the option of enforcing the highest security level available by sending the message as Protected and Registered E-mail.

Regardless of recipient information and options selected by the user, all messages and communication between the customer's connection point to the service with Protectoria are encrypted.

The recipient's e-mail address and mobile phone number are mandatory information in order to send a message through Protectoria.

2.1.2 Sending Protected Messages

When sending protected messages, you have a host of functions that you may choose to enable.

Function	Description / Benefit
Protected and Registered E-mail	A Protected and Registered E-mail is a premium protected message. When this function is used, Protectoria always delivers the message using an authentication notification sent via ordinary e-mail that requires the recipient to enter a PIN-code to open the message and retrieve it from the Protectoria server, regardless of the trust level of the recipient. You may request read and not-read notifications per e-mail and/or SMS. Notifications can be requested to be sent to you either at the time when the message has been delivered or if the message has not been delivered before a certain point in time specified by you.
Protected E-mail	A Protected E-mail is a basic protected message. Protectoria will analyze the availability and trust level of the recipient and decide what security level to use for the message. For recipients to which an authenticated and encrypted channel already exists, Protectoria delivers the message to the e-mail server to which the recipient belongs. For other recipients, Protectoria delivers the message using an authentication notification sent via ordinary e-mail that requires the recipient to enter a PIN-code to open the message and retrieve it from the Protectoria server.
Scheduled Delivery	Enables you to choose the earliest date and time on which the message should be delivered.
Project Reference Code	Enables you to enter a code for the message. The code will appear on the account statement as a way to categorize messages. This enables you to track the cost of multiple messages for a specific purpose, such as a customer, a project or a subject.

PROTECTORIA SERVICE DEFINITION

Message Tracking Reports	For messages that you have sent, you may request a report showing detailed tracking information of the message. This can be presented to 3rd parties that need confirmation that correspondence has taken place. The report can be requested at any time and may be printed or saved as an Adobe PDF file.
User-defined e-mail notification to recipient	When sending protected messages, the recipient will receive an e-mail notification. This option allows you to save a default notification text to accompany notifications to your messages.
Optional send-implementation (e-mail client plug-in)	Customers using the plug-in may choose between and integrated or separate send button in the e-mail client.

2.2 Account Types

Protectoria offers two account types, namely Standalone and Integrated.

2.2.1 Standalone

Standalone enables one or a few people to send protected messages. You may add an unlimited number of users to the account. Any existing e-mail address may be used. Users will use Protectoria Webmail to send and receive protected messages. When you choose this account type, you will be granted immediate access to Protectoria.

2.2.2 Integrated

Integrated enables your users to use Microsoft Outlook with the Protectoria plug-in to send and receive protected messages. Your users will also be given access to Protectoria Webmail to be able to send protected messages when they do not have access to their Microsoft Outlook account. This account type requires that your organization has a Microsoft Exchange dedicated e-mail server. When you choose this account type, Protectoria will contact you following the registration procedure to complete the activation process.

The following table summarizes the main features & differences between the account types.

	Standalone	Integrated
Number of users	Unlimited	Unlimited – depending on price model selected, a charge per user may apply
Interface	Protectoria Webmail	Protectoria Webmail Protectoria Plug-in for MS Outlook
Supported E-mail infrastructure	Any	Microsoft Exchange
User enrollment	Manual, no system administrator involvement necessary	Automatic, system administrator distributes plug-in to selected users using existing server tools

2.2.3 Account administration

Once registered, all customers get access to a web-based administration interface for the service. During registration, you appoint an account owner that will perform the tasks related to your account, such as managing users, settings, etc. The account owner may appoint additional administrators.

3 GETTING CONNECTED

3.1 Registration

Signing up to the service is done on www.protectoria.com or through a unique web link received from a Protectoria sales representative. Once the registration procedure has been completed and payment has been received, you will have the necessary information to start using the service, given that the requirements listed in section 7.3 have been fulfilled. During registration, your credentials such as e-mail address and mobile phone number must be confirmed by Protectoria before access is granted.

3.2 Payment and Account Credit

Protectoria offers two price models, namely pay-as-you-go and pay-per-user. The availability illustrated and clarified below.

	Standalone	Integrated
Pay as you go	Available	Not available
Pay per user	Not available	Available

3.2.1 Pay-as-you-go

With this price model, charges for the service depend on how much it is used. When ordering the service, you are required to add credit to your account using a credit card. Supported credit cards and payment options are shown on the registration page. When you or users on your account use the service, any payable item is charged against the balance of your account. Your account statement can be requested when you are logged in to Protectoria.

3.2.2 Pay-per-user

With this price model, charges for the service depend on how many users are registered in the service at any given time. When ordering, you decide how many users will be using the service initially. These will be charged on the first invoice. Users exceeding the number agreed in the relevant Order will be charged from the time at which they are added to the account and invoiced in the subsequent billing period. New users are registered by Protectoria when the plug-in is installed. Protectoria will count the number of registered users on your account periodically and will invoice accordingly. The customer should remove unwanted users on a regular basis using the web interface provided for this purpose in order to

ensure that only relevant users are invoiced for. Optional chargeable features, such as SMS Notifications, are invoiced after they have occurred at prices listed in the Protectoria price list.

3.3 Account Administration

After the registration procedure has been completed, you get access to your account. Once logged in, you may send protected messages, add additional users, manage your settings, view account statements, manage payments, and so forth.

Customers with their own e-mail server that want to use the plug-in to send protected messages, will first have to install e-mail server prerequisites (i.e. installation of certificate, configuration of connector), then install the plug-in on the individual user's PC. Once plug-ins have been distributed to the users, they will be automatically registered the first time the plug-in logs into the service.

4 PRICING

4.1 Charges

Current Protectoria rates for Pay as you go pricing model (list price) may be [viewed here](#). The rates listed here are an excerpt of the current pay as you go list price. For a complete price list with current list price related to both pay per user and pay as you go, customers may contact their Protectoria sales representative.

4.2 Currency

All items are charged in NOK. Amounts displayed in other currencies are solely for information purposes. Protectoria strives to keep currencies reasonably up to date.

4.3 Account Credit Validity

For maintenance reasons, inactive accounts on a pay-as-you-go price model will expire after 12 months of inactivity. Inactivity occurs when no chargeable item has been debited the account for 12 consecutive months. When an account expires, the account will no longer be available for use. Any remaining account balance for expired accounts is non-refundable.

4.4 Mailbox Size

Protectoria currently does not charge for the size of mailboxes stored in the service, but employs a fair use policy. The service is not intended to function as a data storage service. Protectoria may take necessary steps to remove stored messages in cases where the fair use policy is not respected. Protectoria will take reasonable measures to notify customers before such steps are taken.

5 SECURITY

5.1 Standards and Protocols Employed

Transport Layer Security (TLS) and Secure Sockets Layer (SSL) are international standards for secure communications, and are employed extensively in Protectoria.

- All communications to/from sending/receiving systems to the service are encrypted using TLS or SSL protocols;
- All communications to/from sending/receiving systems to the service are authenticated using TLS or SSL protocols or Protectoria's two-factor authentication;
- RSA 1024 is used as public key encryption algorithm, AES 256 (RC4 128 minimum) is used as symmetrical key encryption algorithm and SHA-1 is used as secure digital signature;
- Notification messages to recipients are sent as unencrypted, regular e-mail;
- Two-factor authentication using the combination of e-mail and SMS is used, depending on the trust level of the recipient and options chosen by the sender. Two-factor authentication is always used when:
 - The sender chooses to send with as Protected and Registered E-mail;
 - The service does not have an encrypted channel to the mail server where the recipient's mailbox resides.

The PIN-code used for two-factor authentication is in the format of minimum 6 numeric characters, and is valid for a limited time.

5.2 Personnel

All Protectoria technical operations personnel have passed extensive background checks and are authorized to operate system components in accordance with Protectoria security policy and internal procedures.

5.3 Threat Protection

The service is protected against a host of threats. To avoid spam and virus in e-mails the service may reject suspicious e-mail messages. The service has a systems design and installed countermeasures that protects it against attacks.

5.4 Login to Webmail

To log into the Protectoria Webmail, a username, password as well as a PIN-code sent to the user's mobile phone (two-factor authentication) is required.

5.5 Configuration Limitations

A maximum limit of 250 recipients or 50 MB per message has been configured. Messages exceeding these limits may be rejected.

5.6 Procedures

Protectoria employs stringent procedures for first-time registration of users and for changes to accounts. Authentication using two or more separate channels is employed throughout.

5.7 Customer's Own Security Measures

Protectoria only secures messages sent through the Protectoria servers, not the customer's own infrastructure. It is strongly encouraged that the customer takes all possible measures to secure its own infrastructure and facilities, including but not limited to buildings, servers, PCs, applications and mobile phones. Using e-mail on mobile phones is convenient; however, please be aware of the security risks associated and take necessary precautions to protect the device and the data stored.

6 CUSTOMER SERVICE

6.1 Contact Options and Response Times

Protectoria assists customers in a number of ways throughout the relationship. Through the online help system and the [searchable knowledge base](#), many questions are answered and most issues are solved.

Should you need help, the following options are possible:

Contact Option	Availability	Response Times
Knowledge base (self service)	24/7	Immediate
Web-based request	24/7	24 Hours
E-mail	24/7	24 Hours
Telephone	24/7	Immediate, maximum 5 minutes

Telephone service is available to customers with Integrated account types only. E-mail and web-based requests are processed within business hours. Business hours are Monday – Friday 0800-1700 CET, excluding public holidays in Norway.

6.2 Authorized Contacts

If an account has more than one user, an Authorized Contact is designated to work with Protectoria's Customer Service. An Authorized Contact can be a technical systems administrator, or a business owner of the system. Users belonging to an account must consult the Authorized Contact when they have issues; the Authorized Contact will be the one who has the administrative privileges in the system to perform changes if required. An account may have up to two Authorized Contacts.

7 TECHNICAL SPECIFICATION

Protectoria employs industry standards and best practises in terms of operating the service and protecting and securing the systems involved in protecting the customer's messages and their content.

7.1 Operational Environment

The following section describes the operational environment of Protectoria.

The operational environment of Protectoria is hosted at Digiplex in Norway. For more information see these pages: www.digiplex.no and www.digiplex.com.

7.1.1 Physical Access Control & Personnel

All directives given by relevant governmental organizations to obtain accreditation of the premises are fulfilled. All servers and network equipment are placed in locked rooms or cabinets. Access to the computer room is strictly controlled. The temperature and humidity are monitored, and a warning to authorized personnel will be initiated if any alarms occur.

7.1.2 Power & Cabling

The main electrical wiring on the premises is engineered to ensure sufficient capacity and independence of critical systems. Uninterruptible Power Supplies with sufficient capacity to ensure a controlled shutdown of the systems are installed on all critical systems. Power and telecommunications lines are sufficiently protected against damage. Network cabling is protected against damage and eavesdropping and fibre optical cables are used where relevant.

7.1.3 Maintenance

All IT equipment is maintained in accordance with the manufacturer's recommendations. Maintenance is performed by authorized personnel only. Equipment that needs to be shipped to a maintenance supplier will not contain sensitive data. A log is established for all maintenance performed on IT equipment. All changes to the IT infrastructure are authorized and logged.

7.1.4 Monitoring

All relevant equipment used in the IT infrastructure is monitored to detect malfunctions and give early warnings on storage capacity shortage. Networks are monitored to detect malfunctions or any attacks from viruses and misuses.

7.1.5 Disposal and Reuse of Media

No IT equipment that will be disposed or re-used will contain sensitive information. No computer media that will be removed or disposed of will contain sensitive information. Procedures prescribed by relevant Governmental organizations are used to remove information from computer media that have been used for sensitive information.

7.1.6 Backup and Restore

Incremental backup is performed each night and a complete backup is performed once a week. Verification of backup is performed weekly. Backup media might be stored in the server room for max 1 week before being moved to local backup safe. Backup media will be moved to remote storage on a quarterly basis. Backup media in the local safe can be stored for 4 months before being reused. Backup media in the remote storage cannot be reused and will be kept for at least 10 years. Restore operation is performed whenever needed. The last 5 versions of a file can be restored from the online or the backup media. Restore tests will be conducted bi-annually. Restore operations are for internal purposes; Protectoria currently does not perform customer-requested restores.

7.2 Maintenance Window

Maintenance, upgrades and introduction of new features may be performed weekly on Saturdays between 0800 and 1200 CET (normal maintenance window) as well as quarterly on the first weekend in a new quarter between Saturday 0800 and Sunday 0800 CET (extended maintenance window). You may experience unavailability or instability within these time periods.

7.3 Prerequisites and supported software

7.3.1 Basic User Prerequisites

In order to send and receive messages, the minimum prerequisites are the following:

- A valid e-mail address;
- Access to the Internet;
- A mobile phone with Short Message System (SMS) capabilities.

Please note that recipients of protected messages also need to possess a mobile phone.

7.3.2 Technical Prerequisites and Supported Software

The following table summarizes technical prerequisites and supported software.

	Standalone	Integrated
E-mail server	Any	Microsoft Exchange versions supporting SSL v.3 or TLS 1.0 and an operational SMTP connector*
Server Certificates	Not required	According to Protectoria requirements
Plug-in	Not supported	Microsoft Outlook 2003/2007/2010 on Windows XP and Windows7

PROTECTORIA SERVICE DEFINITION

Interface language	English	English
Browser	Microsoft Internet Explorer Firefox Opera Chrome	

*An SMTP connector is needed for connecting to Protectoria. The SMTP connector will route protected e-mails to Protectoria with TLS encryption.

7.3.3 Protectoria Certificate Requirements

Server certificate(s) are required for the Integrated account type. The certificate must be issued by a well known source (e.g. similar to issuers in the Windows Root Certificate store). The certificate must support minimum RSA 1024 public key encryption, AES 256-bit (RC4 128-bit minimum) encryption and SHA-1 digital signature. The e-mail server's certificate must be issued by a trusted source and must support minimum 128 bit SSL/TLS encryption. An example of a trusted source is Verisign's Secure Site Pro certificate. Protectoria will determine if the certificate is from a trusted source or not.

There are two ways of registering your certificate with Protectoria, namely through automatic or manual validation. Automatic validation is recommended.

- **Automatic validation.** If your company has installed an Extended validation SSL (EV-SSL) certificate on the domain you want to use with Protectoria, and a second SSL certificate has been issued to your e-mail server from a trustworthy certificate issuer, you may send your certificate to Protectoria by e-mail. Protectoria will then make a validation check of your EV-SSL certificate and perform the authentication and setup.
- **Manual validation.** If your company meets face-to-face with one of Protectoria's sales representatives or distribution partners on your company's premises, and it satisfies the requirements listed above, the only requirement is that you provide our sales staff with your e-mail server's certificate.

8 CONTRACTUAL FRAMEWORK

This Service Definition, General Terms of Use, the Protectoria End-User License Agreement and the Order Form together make up the contract between Message Management AS and the customer.