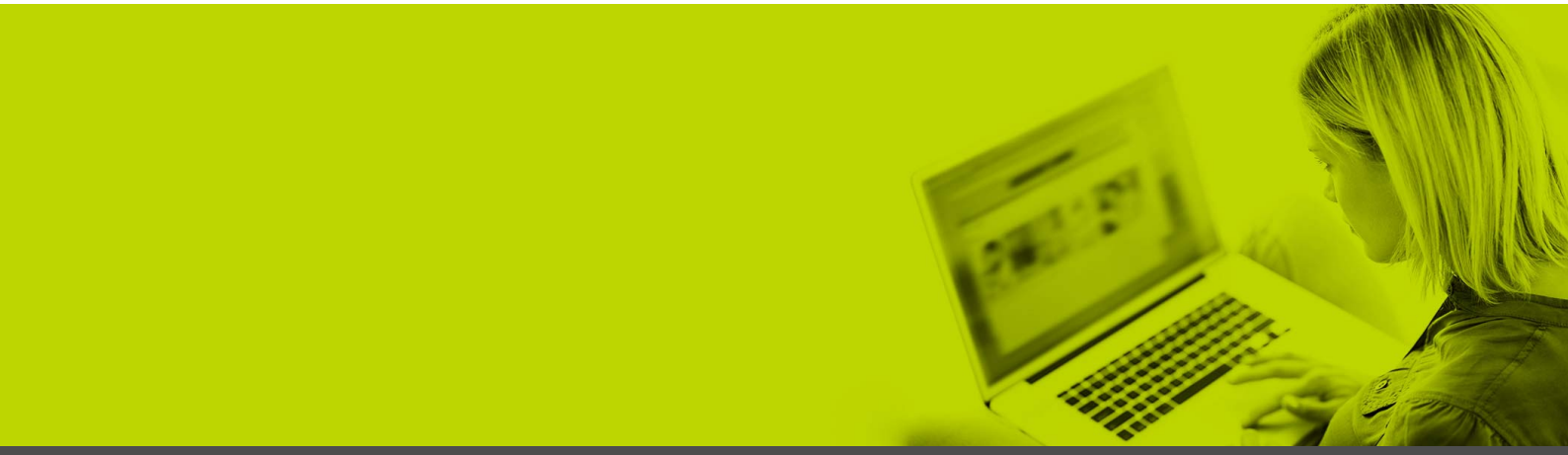
HORNETSECURITY®

23.04.2018



Hornetsecurity Encryption Service

About the Encryption Module

This guide shall support you in configuring and using the Hornetsecurity encryption service. Beginning with the activation and the main configuration, the different encryption methods are explained based on examples. Furthermore, the opportunity of ordering and managing certificates will be explained.

The usage of the Hornetsecurity Websafe for an encrypted communication and keywords inside the email subject will be introduced as well.

Activate the Encryption

1. Navigate to your primary domain in the Hornetsecurity Control Panel.
2. Click on the tab **Encryption** under **Email**.
3. Activate the checkbox **Activate Policy**.

> **Note:** Activating the encryption service will incur a fee.

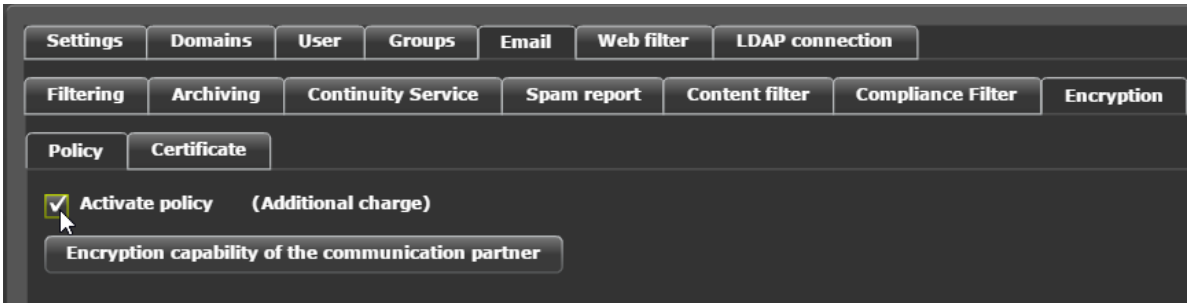


Figure 1: Activate Encryption

Check the Encryption Capability of Communication Partners

You can check the encryption capability of communication partners before you proceed making further configurations on the encryption service.

1. Click on **Encryption capability of the communication partner**.
2. Enter the email addresses to be checked.

Figure 2: Enter communication partners

3. Click on **Check**s to check the encryption capability of the entered email addresses.

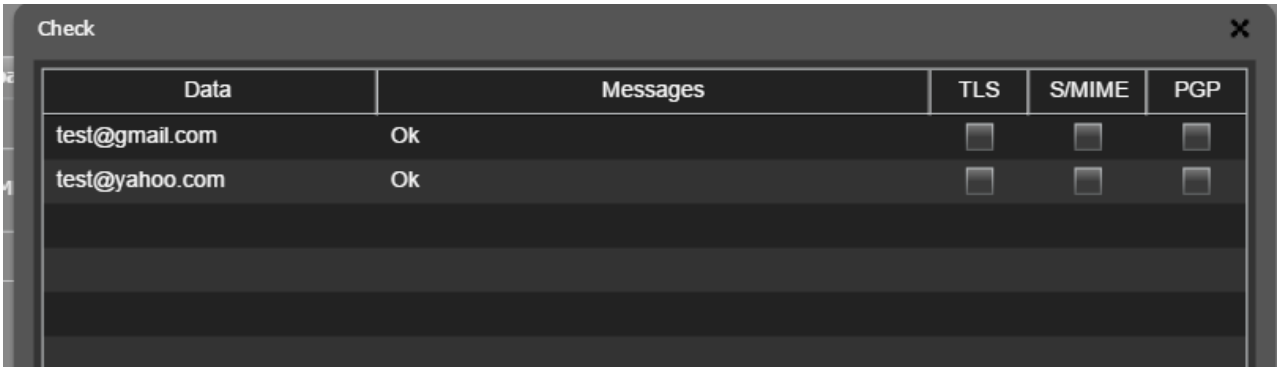


Figure 3: Encryption Capability

Select Encryption Methods

Activate the checkboxes to enable the encryption methods.

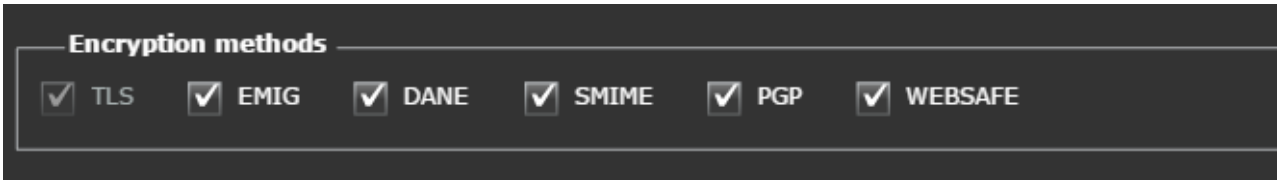


Figure 4: Activate encryption methods

You can select the following encryption methods:

- TLS: Encrypts the email between the servers. This level of encryption is used in every communication.
- EmiG: E-Mail made in Germany encrypts and transfers your messages from your local device to the email server and between the different EmiG providers. In addition, the identities of the providers

are validated against their email certificates and their assigned IP addresses in the EmiG association. EmiG must be booked previously by the customers. After checking the box, it is automatically used for the communication between EmiG users.

- DANE: Is currently in preparation for rollout. If you are interested contact the support for a quick implementation.
- PGP: Is a hybrid method to sign and encrypt emails. It is based on the “web of trust”. Instead of the hierarchical approach of certificate authorities, users are validating their keys among each other. S/MIME: Is a standard for signing and encrypting MIME data through a hybrid encryption procedure. The certificate authority (CA) assures the validity of the email address and the sender.
- WEBSAFE: Is a fallback encryption method. (See: *Websafe* on page 12, for detailed information)

Note: After the activation of the encryption service, you can use PGP, S/MIME and WEBSAFE in order to define certain encryption policies. However, you should define who is communicating end-to-end with each other. TLS and EmiG are used automatically, if the communication partner supports these encryption methods.

Order of Encryption Methods

You can use several encryption methods at once. They are processed in the following order:

S/MIME # PGP # EmiG # (DANE) # TLS # Websafe

Additionally, you can combine the different encryption methods. (See: *Combination of encryption methods* on page 9)

Subject Tagging for Encryption

For a simple handling of encrypted emails, you can tag them in the email subject. The tag content can be chosen freely.

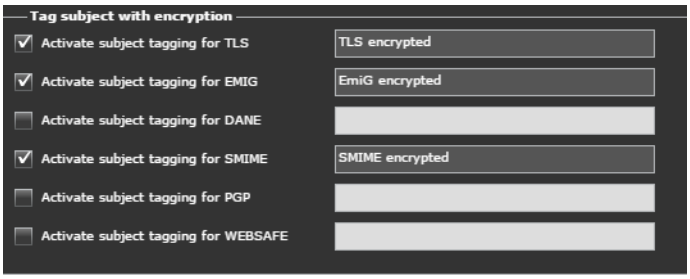


Figure 5: Subject tagging

Set Deviating Encryption Policies

Deviating from the default encryption methods, you can define rules for certain incoming and outgoing emails.

Note: You can change the rule type for outgoing emails. The Types **Advanced**, **Email Header** and **Email Body** are available. Furthermore, you can use regular expressions in the definition of rules. For more information about regular expressions and how to use them, see the Compliance Filter guide

1. Click on **Add** in the policy section.
2. Select the direction:
   - Incoming
   - Outgoing
3. Enter sender and/or receiver. You can enter domains, groups of users or individual email addresses.
4. Select an action for your rule.

   You can select **allow unencrypted** or **always encrypt**. Activate the checkboxes with the desired encryption methods. You can select TLS and DANE for incoming emails. For outgoing emails, you can use all previously selected encryption methods.

   The figure below shows a policy defined for incoming emails of the domain **domain.com**. All emails are encrypted by the task **"Encrypt always"** using the encryption method TLS. (This policy has no function and is only used for demonstration purposes, since TLS is used for all incoming and outgoing emails by default, if the communication partner supports this encryption method.)

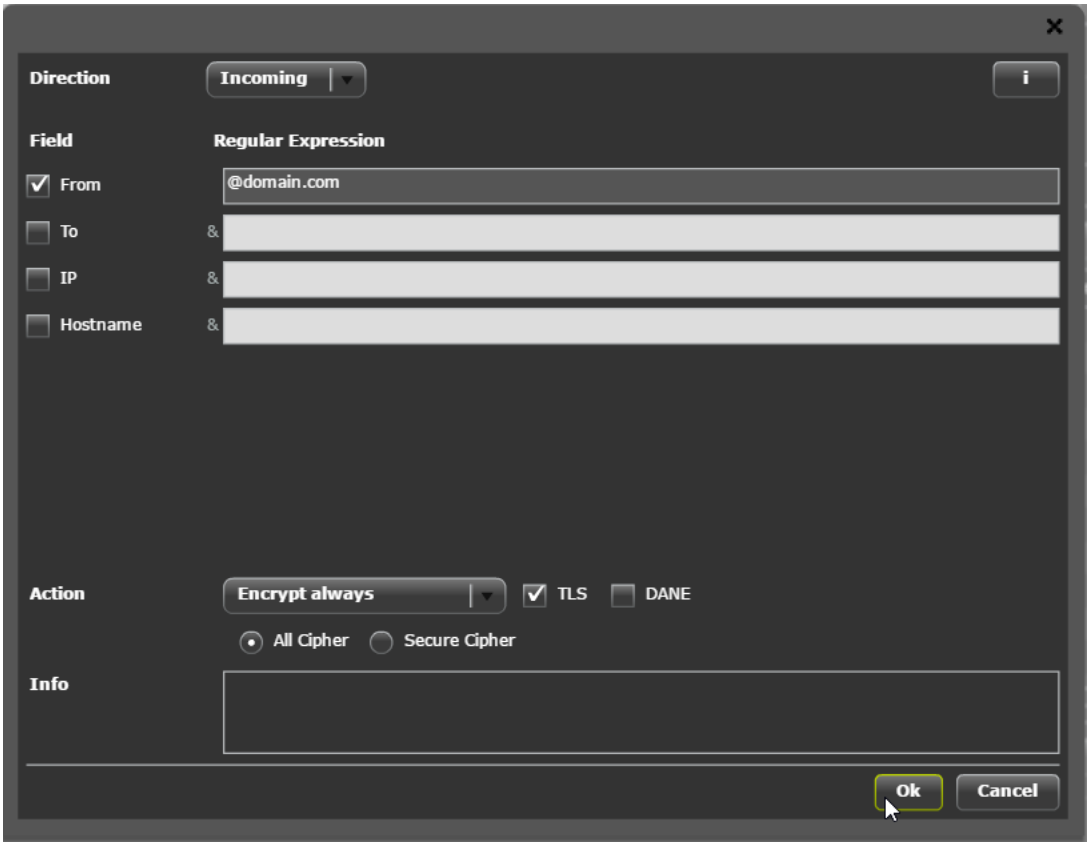


Figure 6: Encryption policy for incoming emails

The figure below shows a policy defined for emails from secret@mycompany.com. All outgoing emails from that address are encrypted with TLS and as a fallback Websafe is activated.

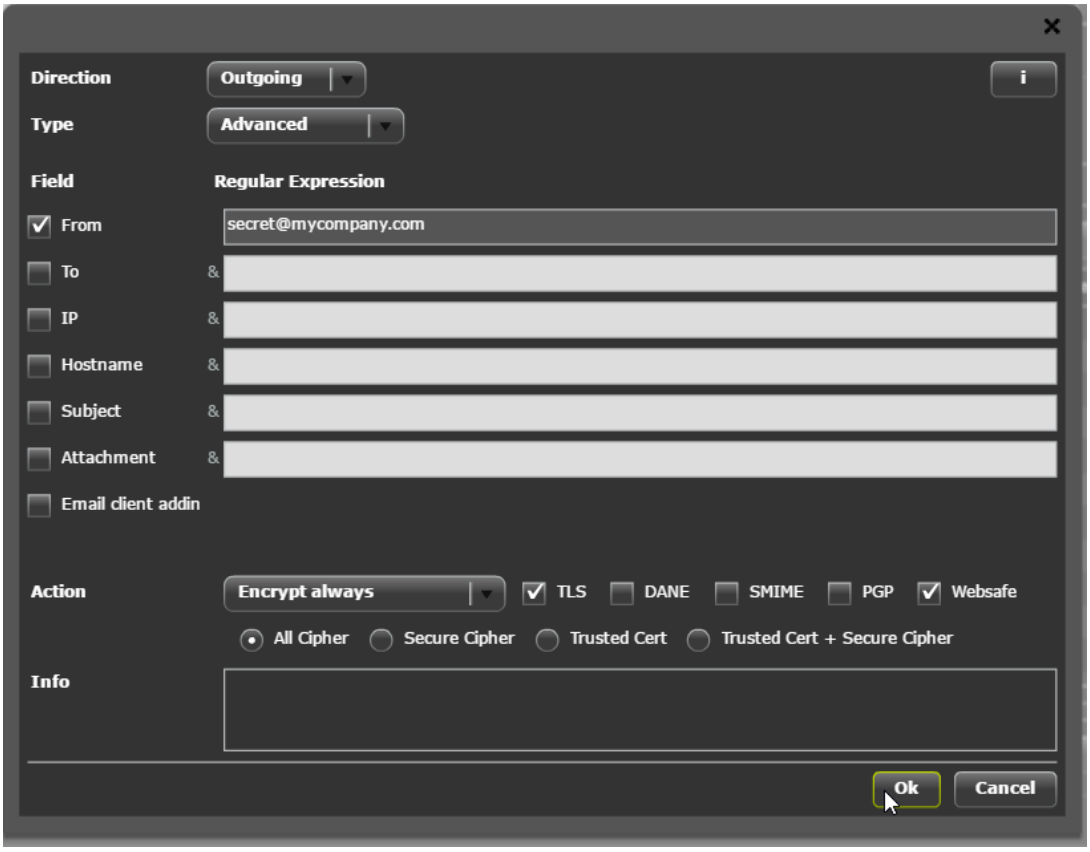


Figure 7: Encryption policy for outgoing emails

The figure below shows a policy defined to search the email header of outgoing emails for the phrase **secret product name**. If the defined expression occurs, the email is encrypted with TLS and if the communication partner does not support TLS, the email is sent to the Websafe.

Note: The expression is found even if it's surrounded by text. Therefore, **ABCsecret product nameDEF** will match as well.

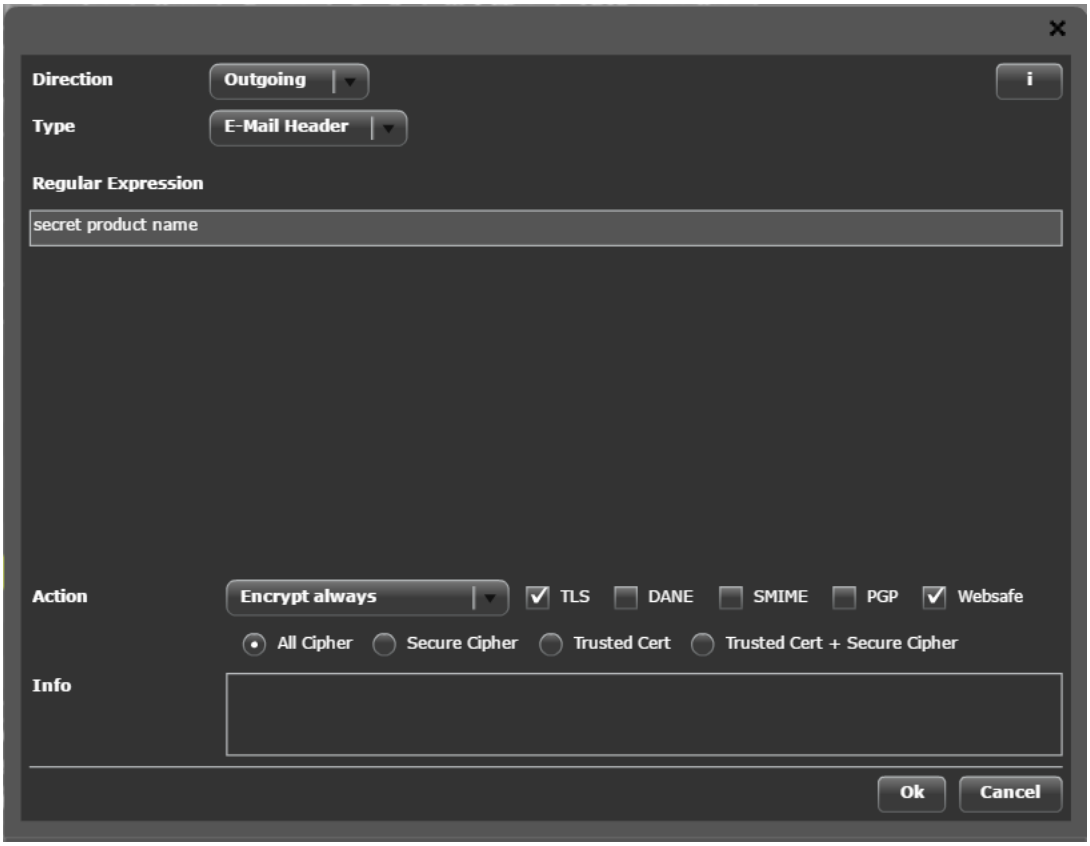


Figure 8: Encryption Policy for the email header or body of outgoing emails

All rules are collected in a list and processed from top to down. If you want to arrange the rules in a specific order, select a rule and click on the green arrows as shown in the figure below.

Note: If a policy matches, the execution stops and no other policy is applied.

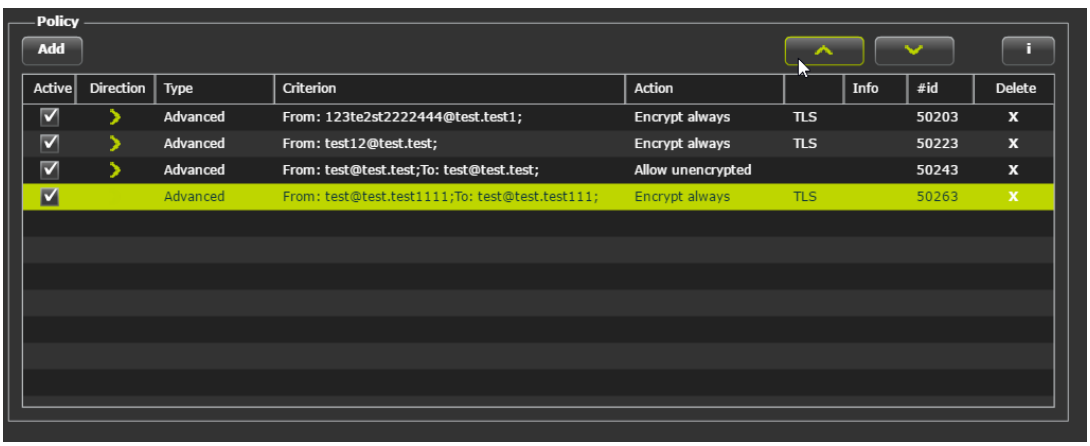


Figure 9: Policy order

Combination of encryption methods

In principle it is possible to combine the different encryption methods. The following table provides the combination possibilities. An x indicates that the encryption methods are compatible with each other.

Table 1: Encryption combinations

Encryption Method	TLS	EmiG	S/MIME	PGP	DANE	WEBSAFE
TLS	-	-	x	x	x	-
EmiG	-	-	x	x	x	-
S/MIME	x	x	-	-	-	-
PGP	x	x	-	-	-	-
DANE	x	x	-	-	-	-
WEBSAFE	-	-	-	-	-	-

In addition, you can always activate the Websafe to have a fallback, if the communication partner does not support any other encryption method.

The figure below shows a policy defined for outgoing emails from mydomain.com to communicationpartner.com. All emails are encrypted with both TLS and S/MIME.

Note: Check if your communication partner supports the preferred encryption methods before activating them (see: *Check the Encryption Capability of Communication Partners* on page 2)

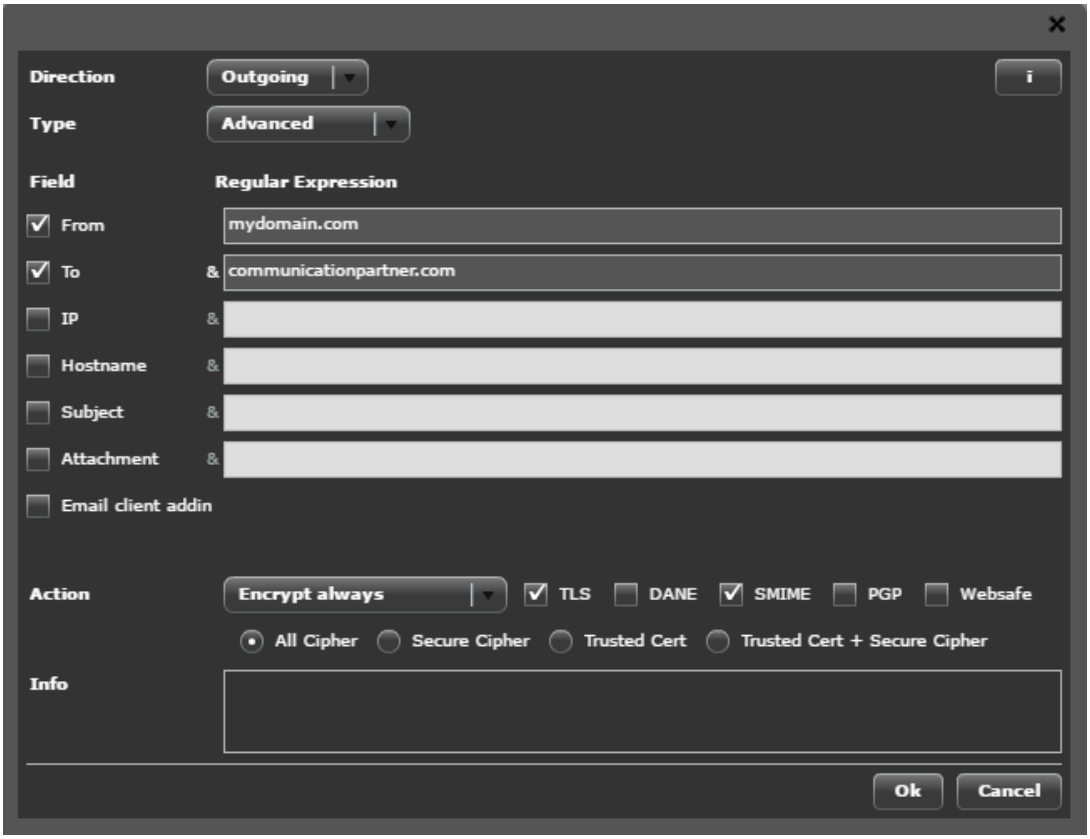


Figure 10: Combination of TLS and S/MIME

If you select all possible encryption methods for one policy, the applicable emails will be encrypted in the order shown in *Order of Encryption Methods* on page 4. All possible combinations are applied automatically.

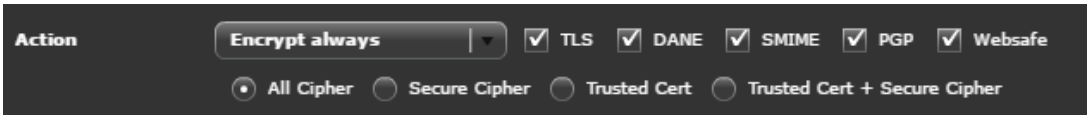


Figure 11: Selection of all encryption methods

Certificates

You will find the administration of certificates under Certificate. Here you can order and manage S/MIME certificates for users of the selected domain.

Ordering Certificates

1. Select the tab **certificate**.
2. Select a user from the list.

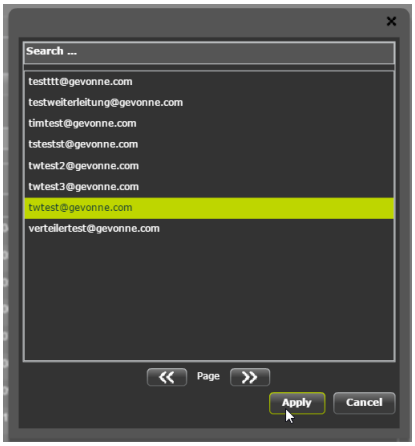


Figure 12: User selection for certificates

3. Enter the first and last name of the user

> **Attention:** Be sure to enter the correct information before ordering the certificate. It is only valid as a signature if the entered name is valid.

4. Click on **Order**, to complete.

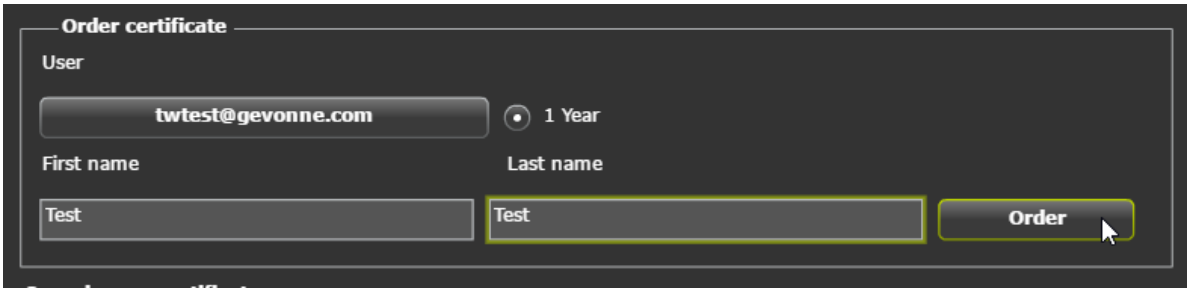


Figure 13: Order a certificate

Certificate settings

In the certificate overview you can define for each certificate to handle the signing and/or encrypting of emails. By default, signing and encrypting is enabled.

Furthermore, you can activate a subscription for the certificate. Certificates with an active subscription will automatically be renewed 29 days before expiration. The subscription is activated by default

Note: If you do not want a subscription, deactivate it at least 30 days before renewal.

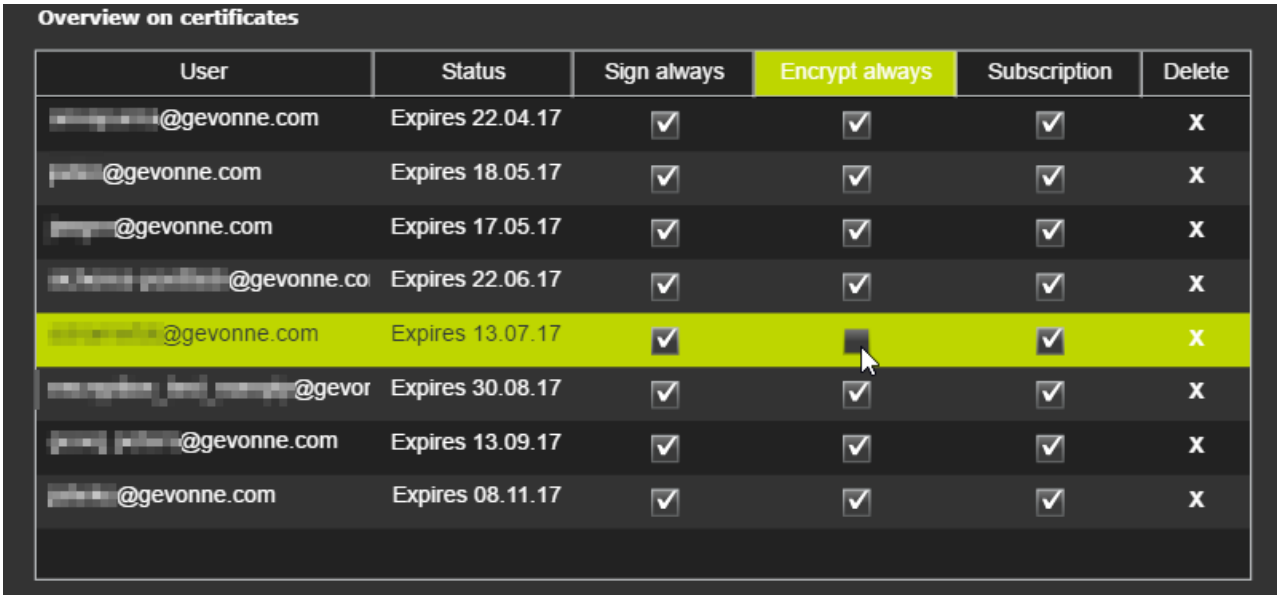


Figure 14: Certificate overview and options

Websafe

The Hornetsecurity Websafe is a method to encrypt the email communication with partners using no encryption technologies. The outgoing emails are sent to the Websafe and saved. After that, the communication partner receives an email with login credentials, but will need an additional PIN to unlock the personal Websafe. The email sender must provide the PIN on a separate communication channel (phone, text message, fax). With the PIN and the login credentials, the user can access his personal Websafe.

Note:

A Websafe account is automatically created and can be used for additional Websafe communication.

As soon as the communication partner opens a new email in the Websafe, the sender receives a confirmation message that the email has been read.

Before configuring the Websafe, you must activate it in the encryption methods. (see: *Select Encryption Methods*)

Setting up the Websafe for specific Communication Partners

1. Click on **Add** in the tab **Encryption** under **Policy**.
2. Select **Outgoing** as direction.
3. Activate the checkbox **To** and insert the receiver into the field.
4. Select **Encrypt always** as action and activate the checkbox Websafe.

If no other encryption method can be used for the email communication, Websafe will be used.

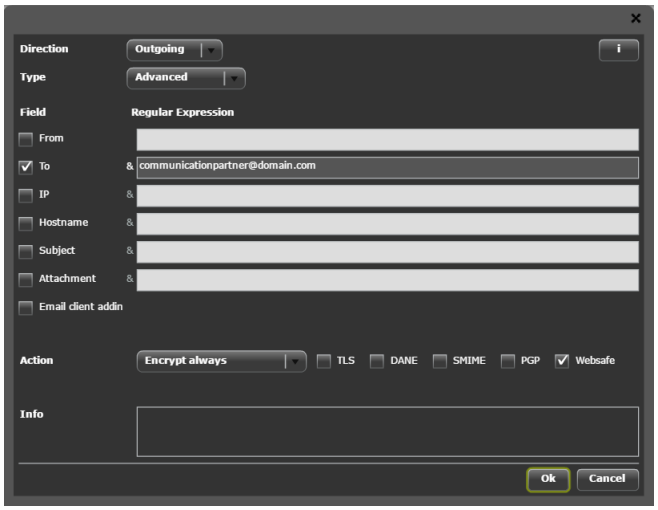


Figure 15: Activate websafe for a specific communication partner

Encrypt Emails with Websafe as Fallback

You can use the Websafe to make sure that all outgoing messages will be encrypted.

1. Click on **Add** in the tab **Encryption** under **Policy**.
2. Select Outgoing as direction.
3. Check the boxes **From** and **To**.
4. Insert **.*** in both fields.
5. Select **Encrypt always** as action and check the box **Websafe**.

Outgoing emails that are not encrypted by any other method, are sent to the Websafe.

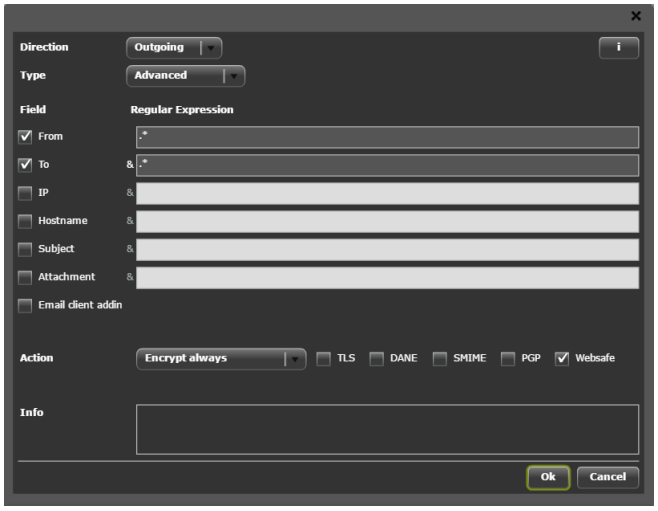


Figure 16: Websafe for all unencrypted emails

Enable Websafe Encryption through the Email Subject

You can define a rule to encrypt emails by setting a keyword in an email's subject.

1. Click on **Add** in the tab **Encryption** under **Policy**.
2. Select **Outgoing** as direction.
3. Activate the checkbox **Subject**.
4. Enter the keyword **WEBSAFE** in the field.
5. Select **Encrypt always** as action and activate the checkbox **Websafe**.

Entering **WEBSAFE** into the email subject, results in encrypting the email over the Websafe.

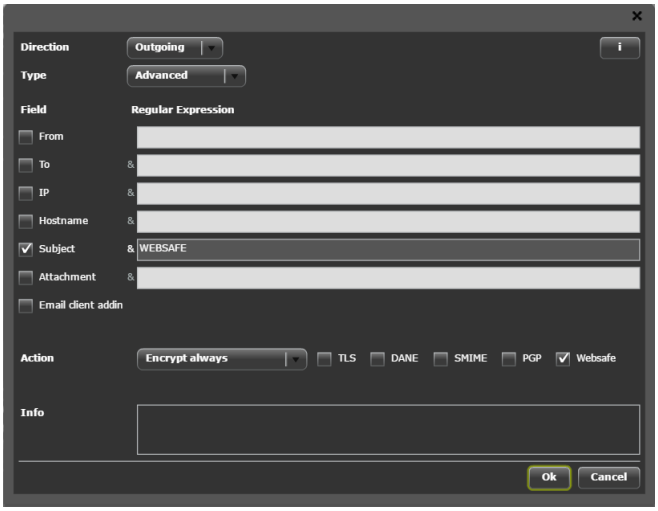


Figure 17: Websafe as subject keyword

Websafe Templates

You can select templates for the sender notifications, the recipient notifications and the website of the Websafe activation.

Note: Partners can create and change templates. (See: *Control Panel Manual: Templates*)

Selecting Websafe Templates

1. Navigate to **Websafe Templates** under **Encryption**
2. Select the desired templates from the drop-down menus.

Figure 18: Selecting Templates

Using Keywords in the email subject

You can use the following keywords in your emails subject to trigger specific actions:

- CRYPT: The email is encrypted with the activated encryption methods in the defined *order of encryption methods*.

> **Note:** The keyword **CRYPT** has no function.

- NOCRYPT: The email is sent unencrypted. SIGN: The email is sent signed.
- NOSIGN: The email is sent unsigned.
- WEBSAFE: The Websafe is used for the encrypted communication. (Needs policy definition in Control Panel: See *#unique_15/unique_15_Connect_42_img_WEBSAFE* on page 15)

> **Important:** You must write the keywords in capitals.