

NORMAN[®]

Sample Sharing Initiative



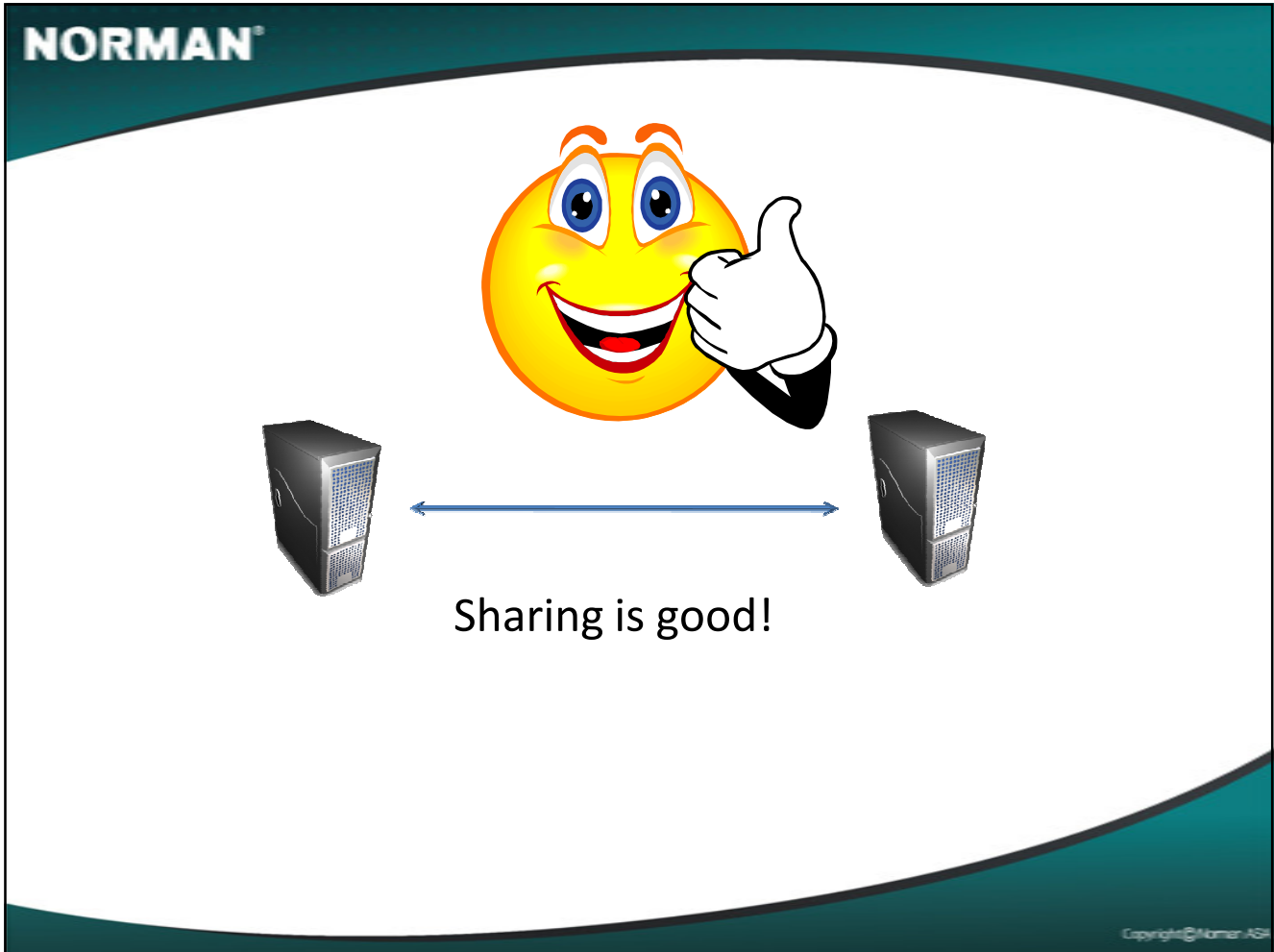
Trygve Brox
Lead Programmer – Internal Systems

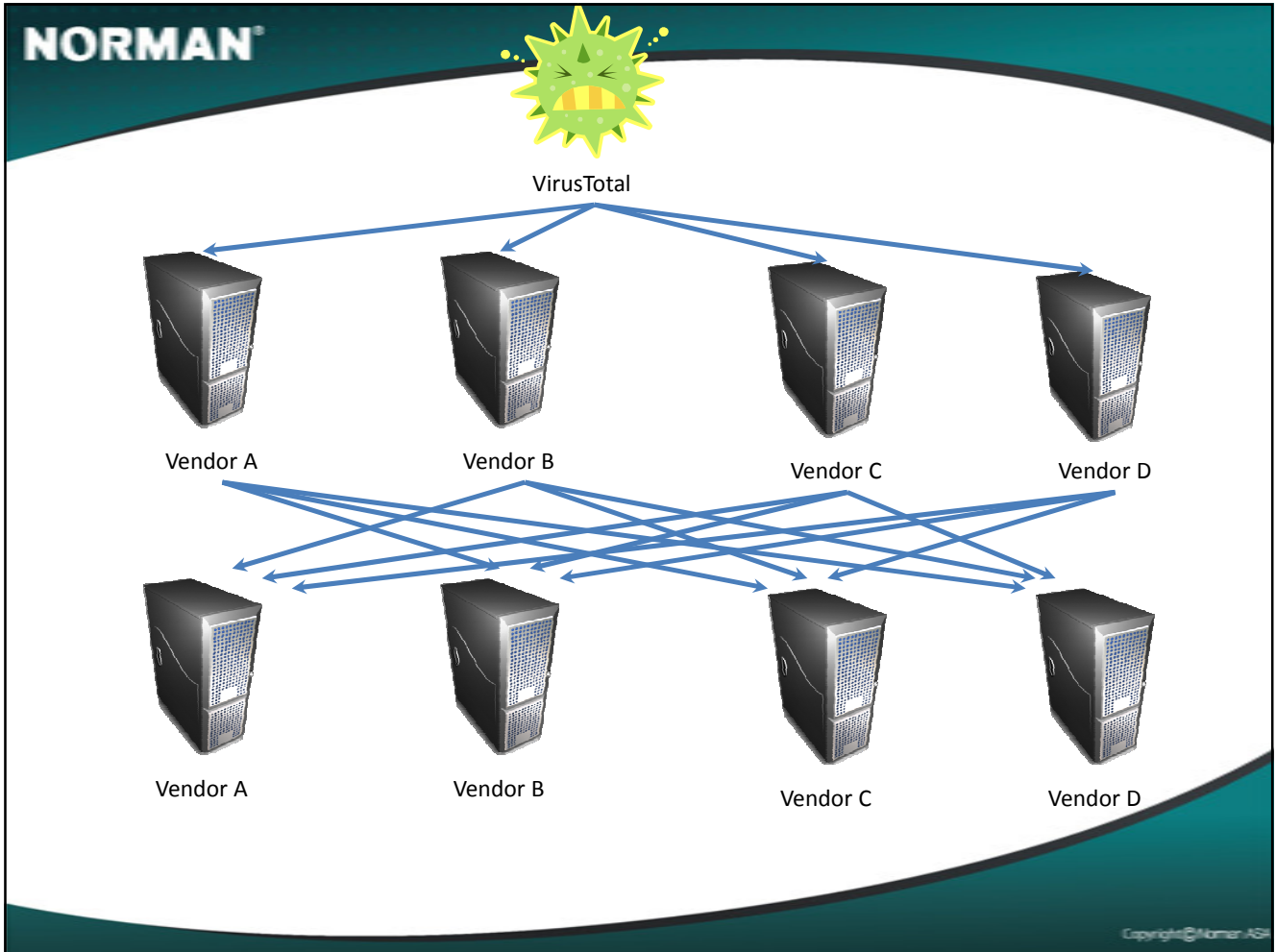
CARO 2010 Workshop
May 26 and 27, 2010
Helsinki, Finland

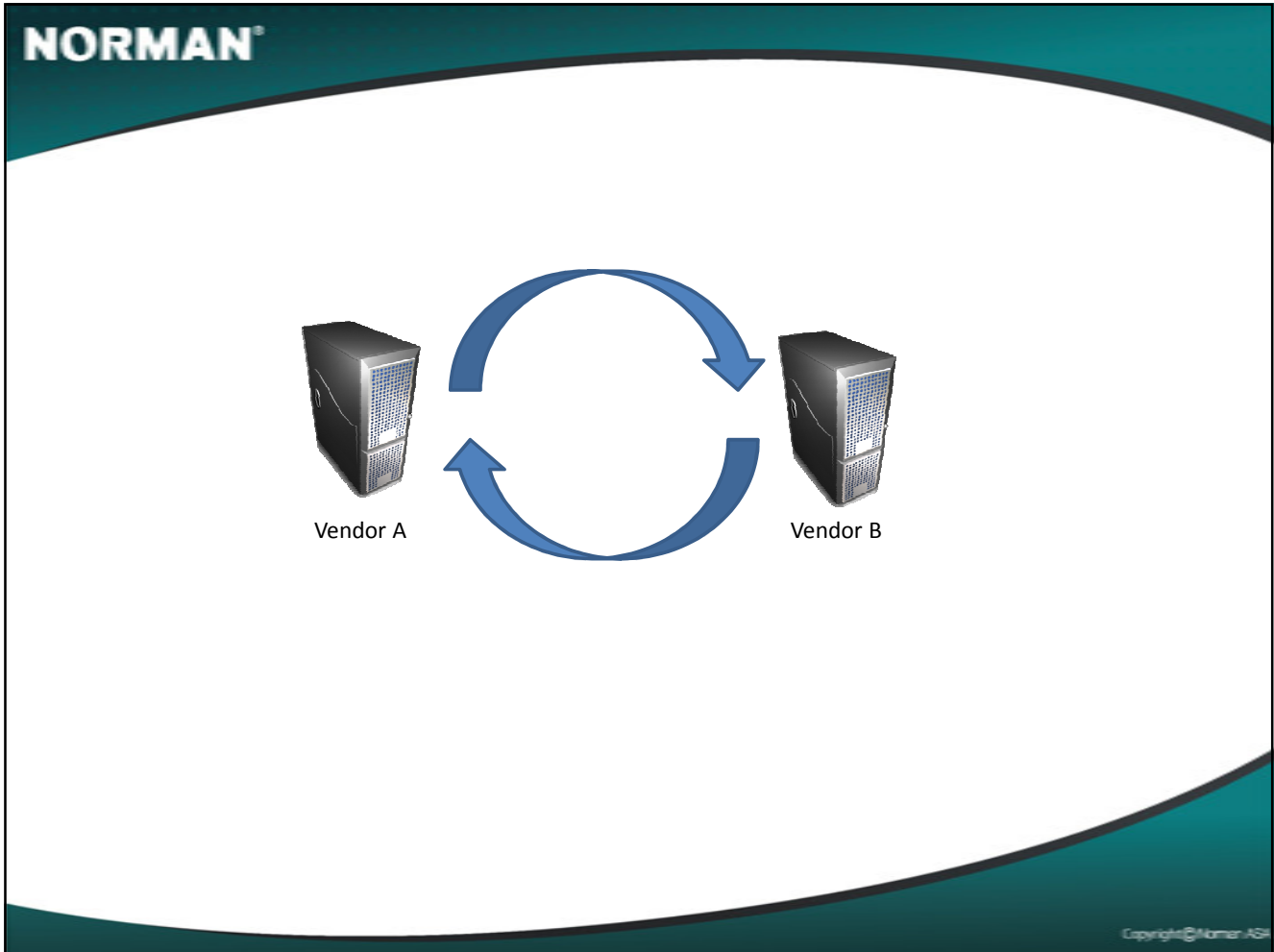
Righard Zwienenberg
Chief Research Officer



Copyright © Norman ASA



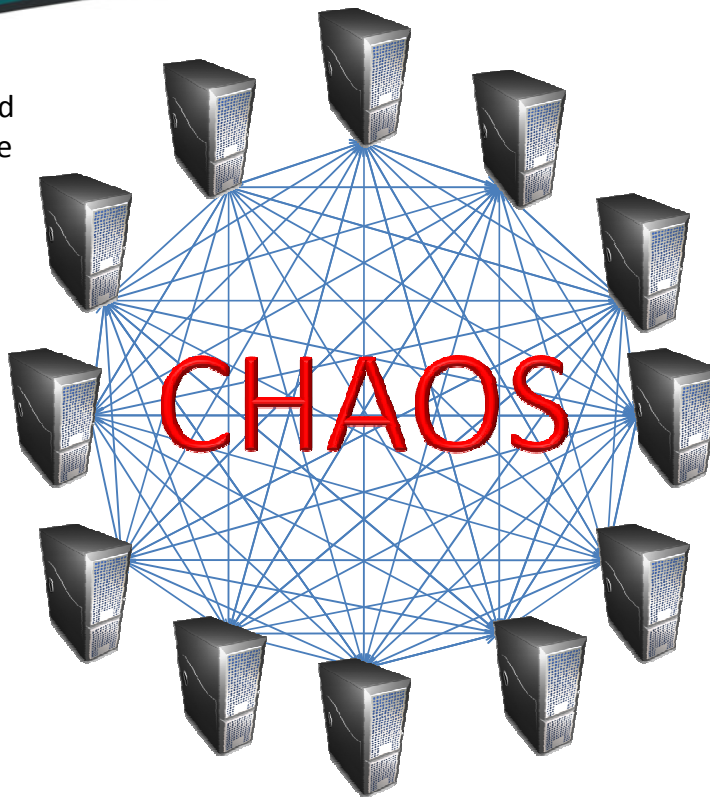




Copyright © Norman ASA

NORMAN[®]

Sample sharing and
the mess we create
today

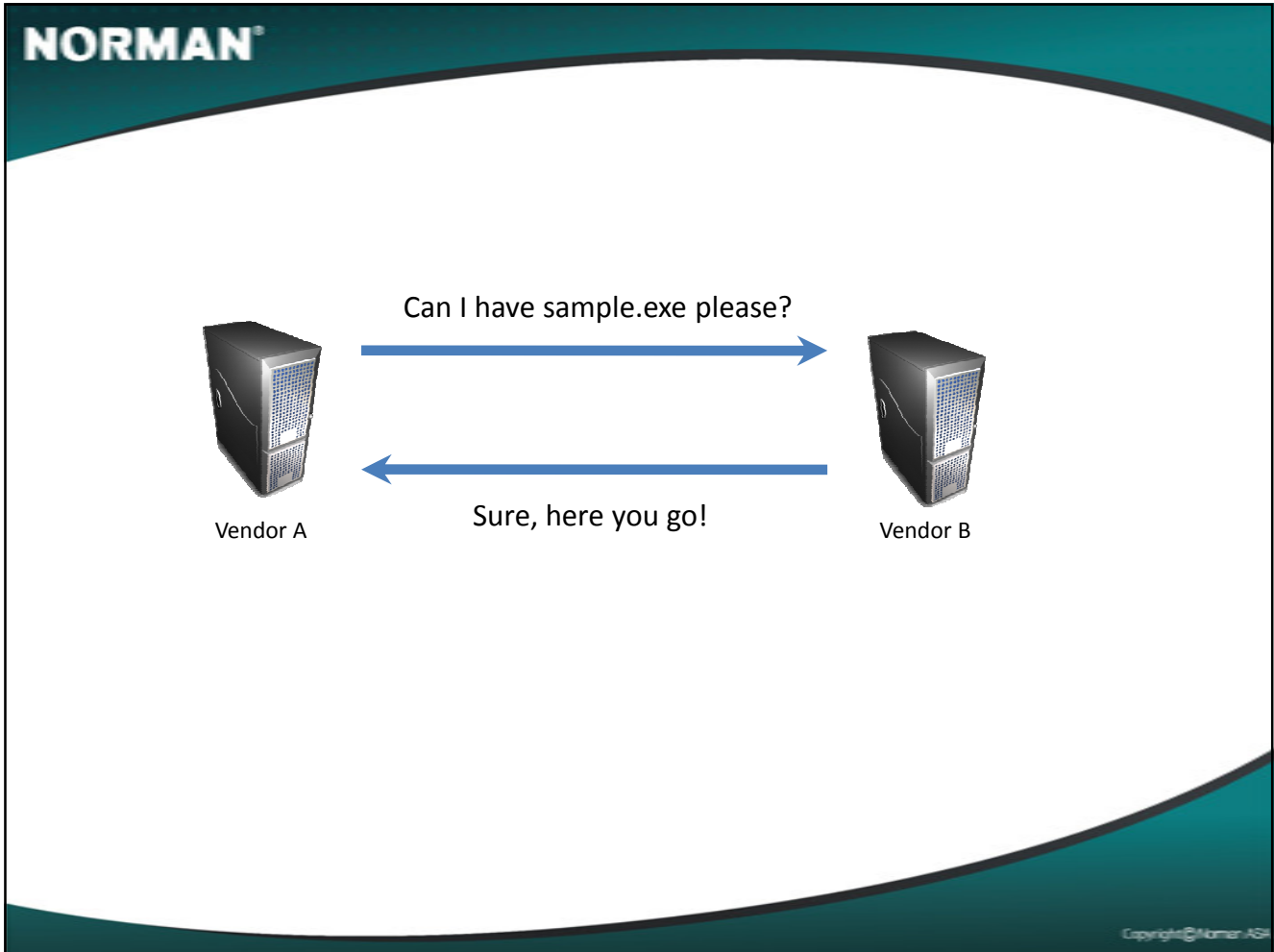


- Multiple duplicates
- Slow distribution

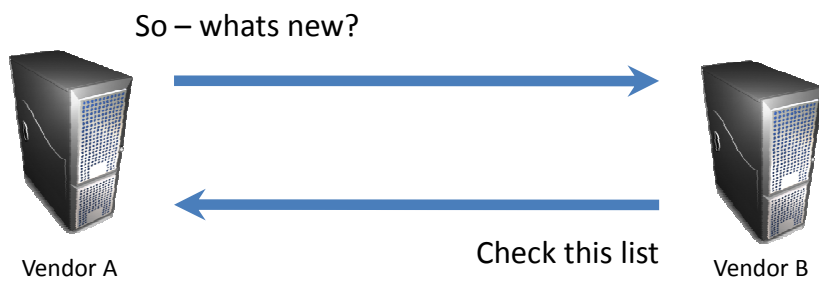
Waste of

- Bandwidth
- Storage space
- Processing power
- Human resources

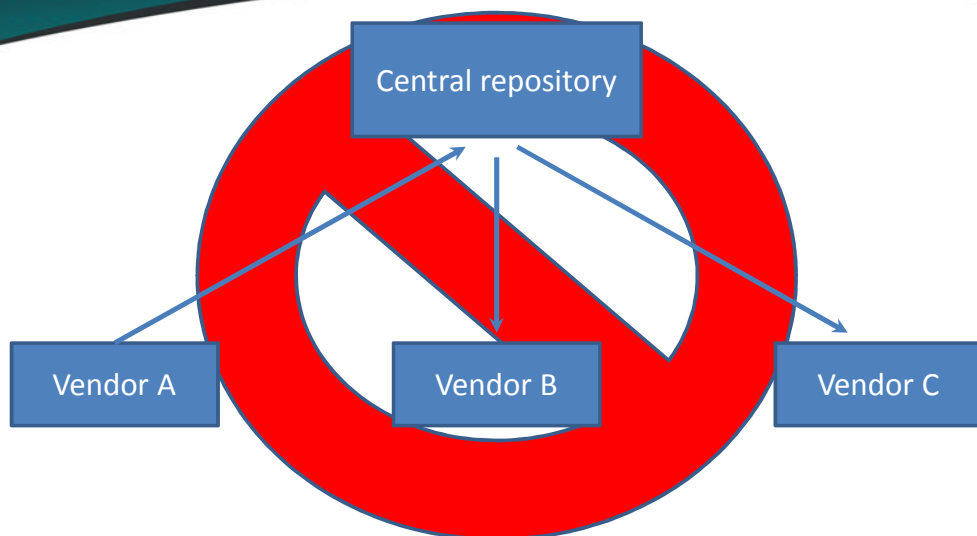
Copyright © Norman ASA



NORMAN



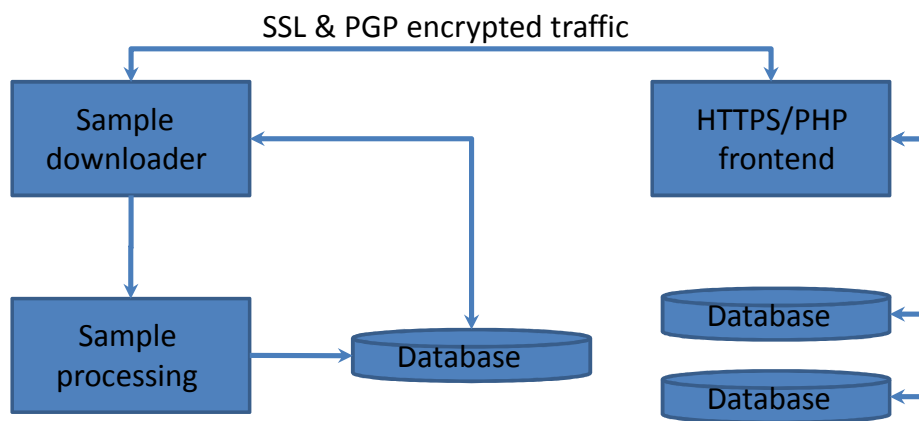
Copyright © Norman ASA

NORMAN[®]

A central sample repository might be better, but there are too many challenges

- Who would maintain it?
- Who would pay for it?
- Is there such a thing as a neutral third party?

Copyright © Normar, ASH

NORMAN[®]

Client-server solution for sharing samples.

The server provides a list of shared samples, and the client downloads new files only.

NORMAN[®]

For our project we have made the following choices:

Software:

Apache, MySQL and GnuPG – Open Source and well known.
Can be installed on both Linux and Windows.

Network protocols:

HTTPS – Security for free, and completely platform independent

Script language:

PHP & Curl – Well known and very simple

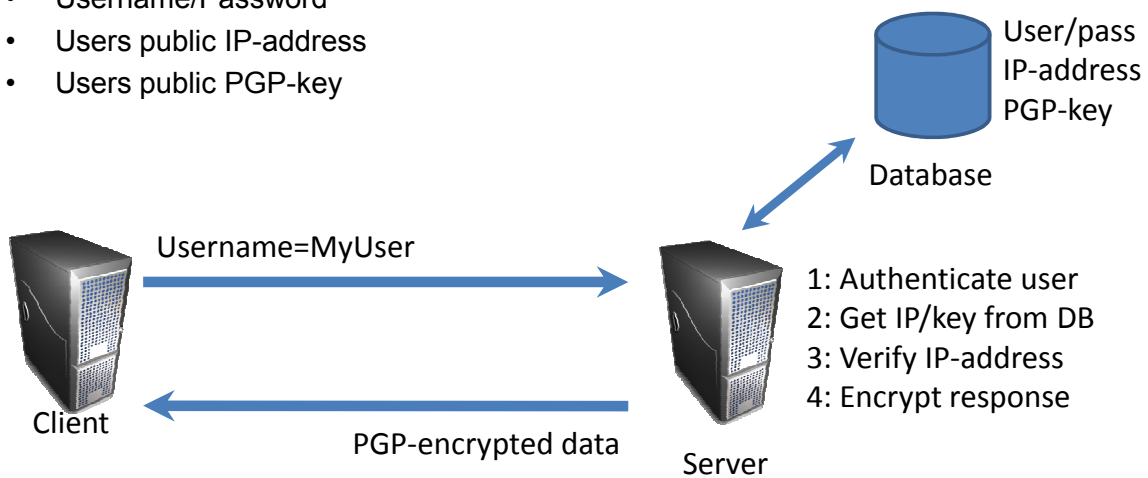
We will provide PHP-classes, example-code and documentation.

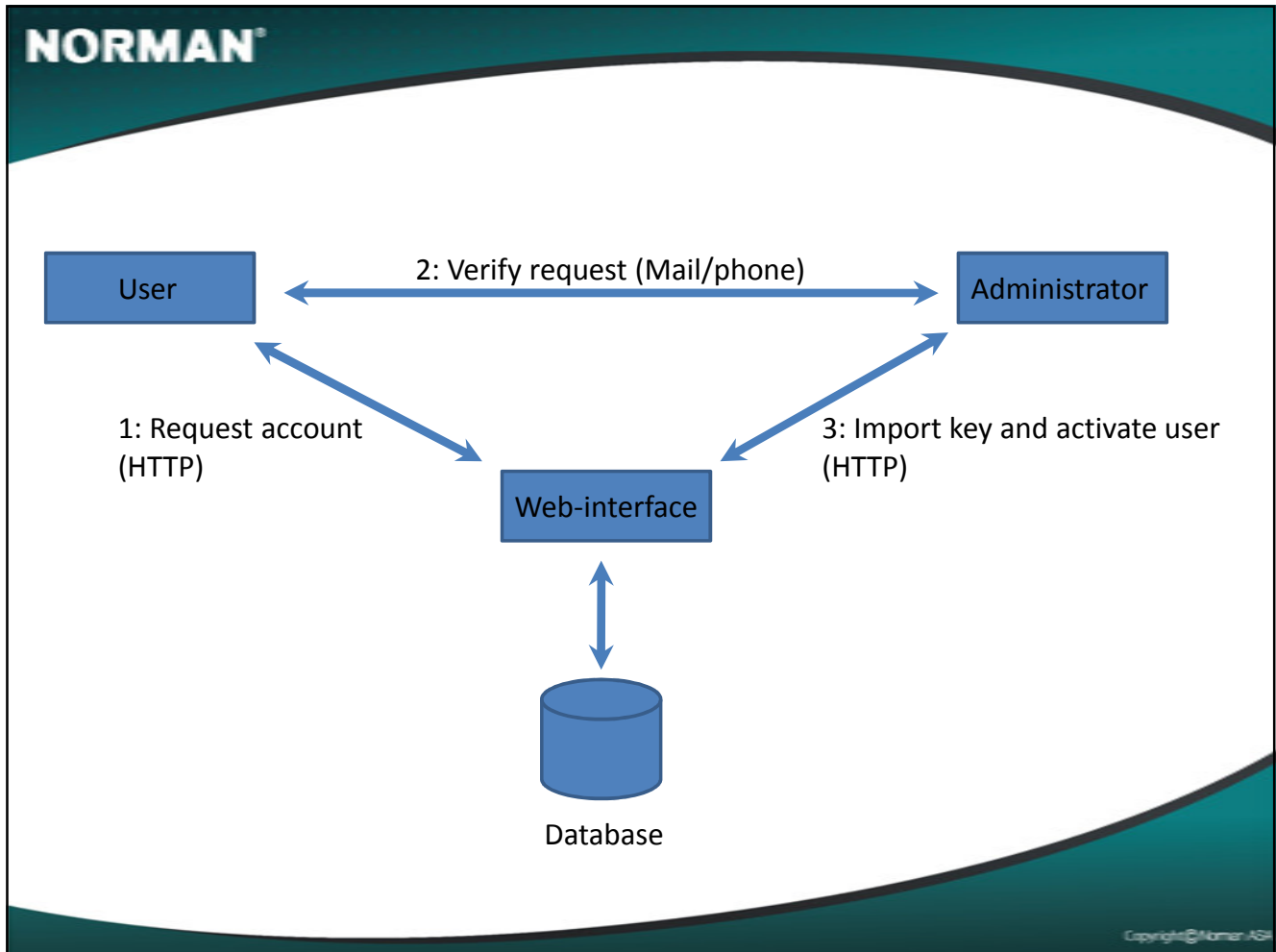
The supplied code can be used with minimal effort, or you can make your own implementation using your favourite language.

NORMAN[®]

All users must be registered with:

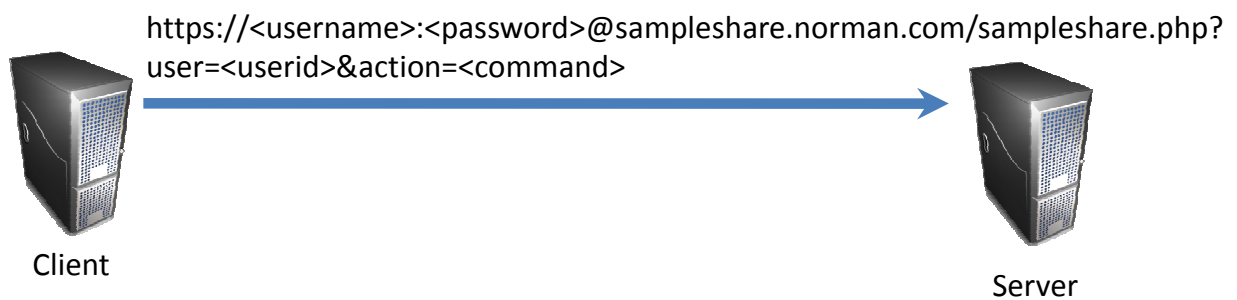
- Username/Password
- Users public IP-address
- Users public PGP-key



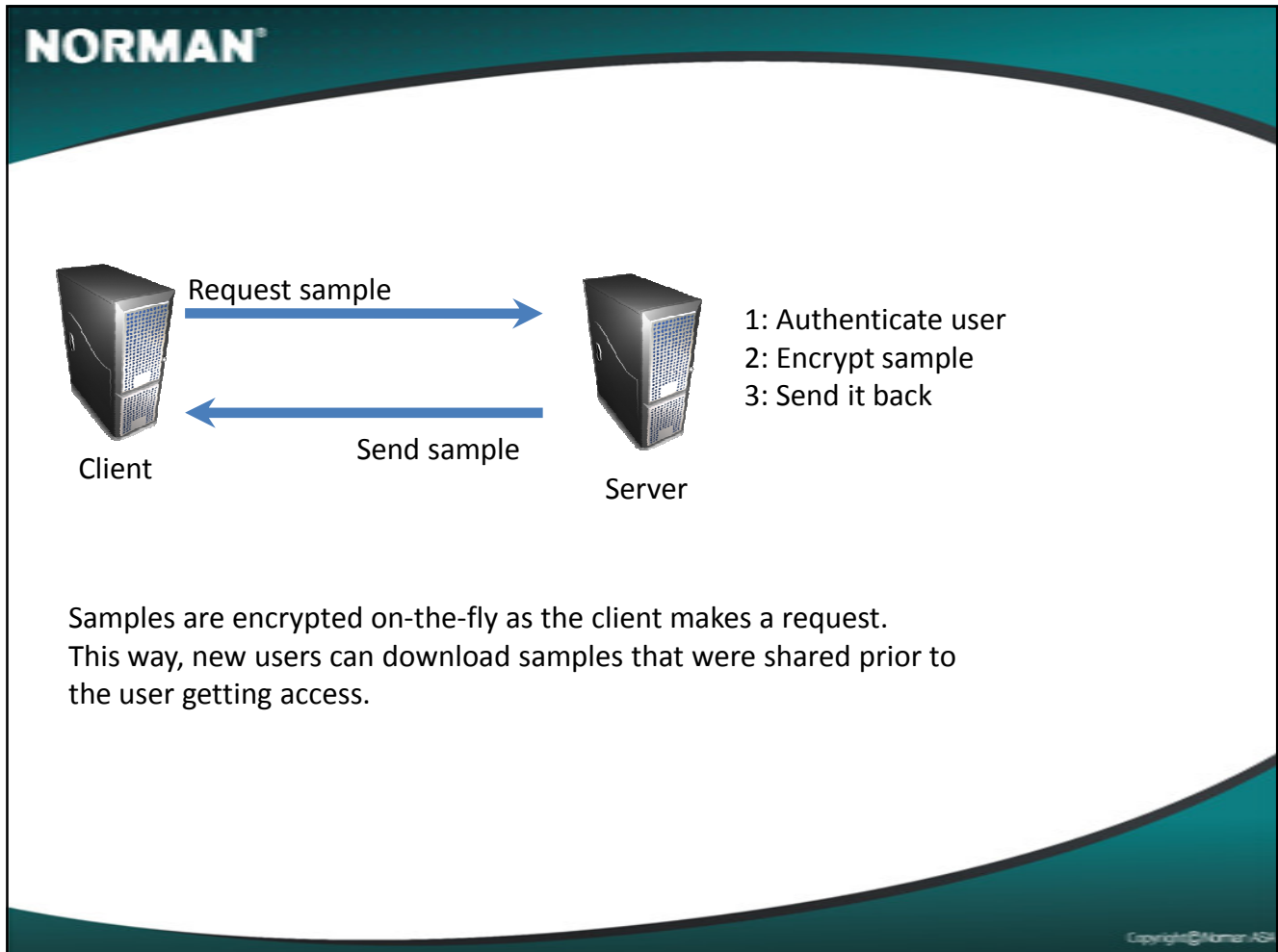


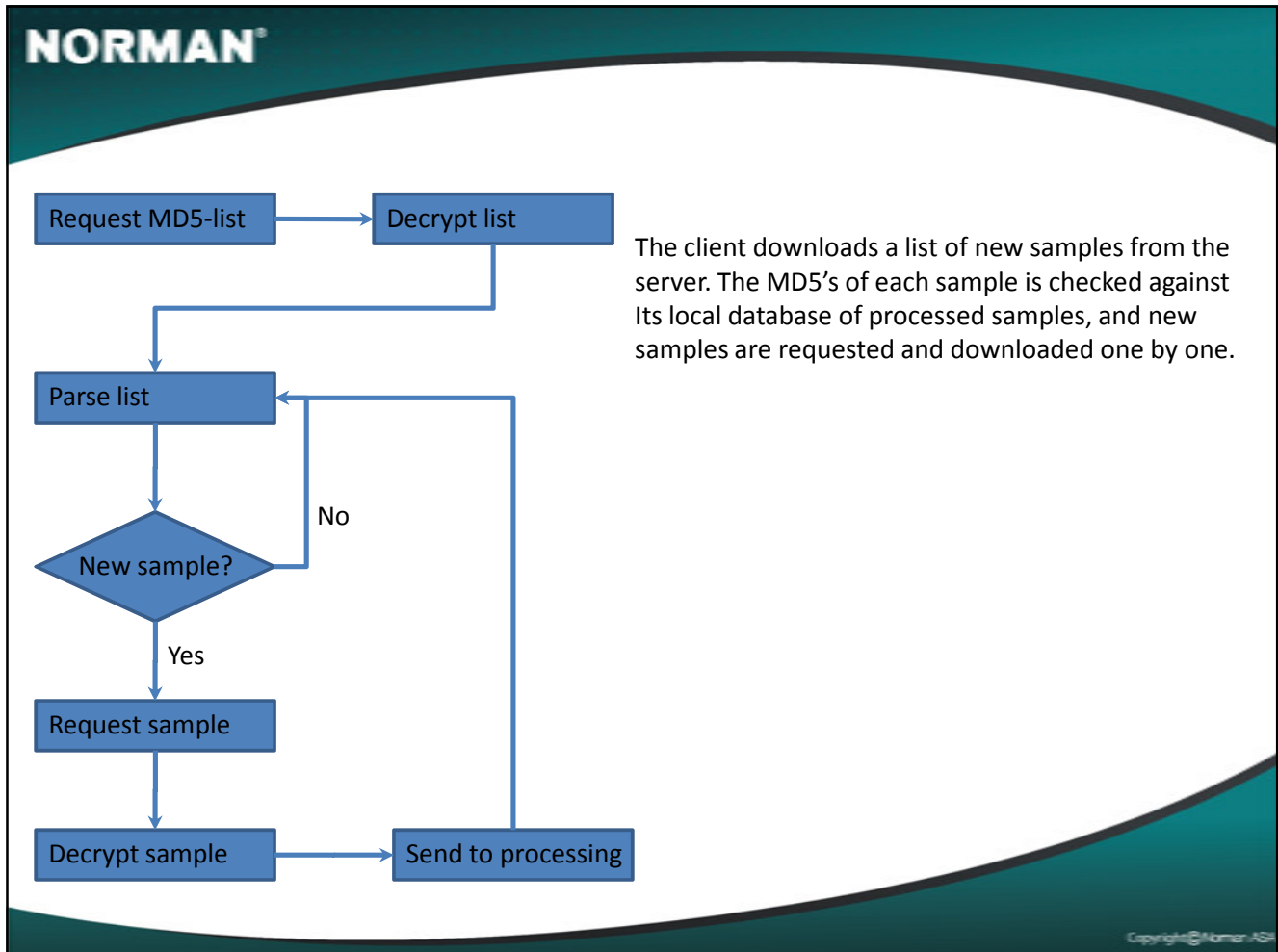
NORMAN[®]

All interaction with the server is done with get-requests to a web-interface



Send commands using Curl, Wget, Winsock, whatever in automated scripts, or even your browser to make manual requests





NORMAN[®]

Client example code

```
<?php
include('sampleshare.inc');

$share = new SampleShareObject();

$share->set_dates("2010-04-05 00:00:00","2010-04-06 00:00:00");
$share->set_http_user("<user>","<password>");
$share->set_url("sampleshare.norman.com/auth/sampleshare.php");
$share->set_download_directory("d:/sampleshare/incoming");

$share->get_list();

echo "$share->md5count samples found. Starting download.. \r\n\r\n";

foreach($share->md5list as $entry) {
    /* Your code to determine if a file should be downloaded */
    if($download_this_file==true) $share->get_file($entry["md5"]);
}
$share->print_avg_speed();

?>
```

NORMAN[®]

Client output – local network

C:\PHP>php sampleshare.php

Requesting files shared between 2010-04-05 00:00:00 and 2010-04-06 00:00:00..

300 samples found. Starting download..

Downloaded 521.74KB in 0.453 seconds at 1151.75KB/sec

Downloaded 21.19KB in 0.046 seconds at 460.62KB/sec

Downloaded 41.89KB in 0.062 seconds at 675.70KB/sec

Downloaded 42.25KB in 0.062 seconds at 681.53KB/sec

....

....

Downloaded 58.08KB in 0.094 seconds at 617.87KB/sec

Downloaded 15.39KB in 0.047 seconds at 327.40KB/sec

Downloaded 65.23KB in 0.093 seconds at 701.35KB/sec

Downloaded 926.65KB in 0.733 seconds at 1264.19KB/sec

Downloaded 14.96KB in 0.046 seconds at 325.30KB/sec

Downloaded 406.00KB in 0.359 seconds at 1130.91KB/sec

Downloaded 568.58KB in 0.453 seconds at 1255.14KB/sec

Downloaded 109.83KB in 0.14 seconds at 784.52KB/sec

Downloaded 2.65MB in 1.95 seconds at 1390.03KB/sec

Downloaded 300 files/140.60MB in 76 seconds at 1.85MB/sec

NORMAN[®]

Client output – remote download

```
C:\PHP>php sampleshare.php
Requesting files shared between 2010-04-05 00:00:00 and 2010-04-06 00:00:00..
300 samples found. Starting download..
```

```
Downloaded 521.74KB in 1.107 seconds at 471.31KB/sec
Downloaded 21.19KB in 0.078 seconds at 271.65KB/sec
Downloaded 41.89KB in 0.125 seconds at 335.15KB/sec
Downloaded 42.25KB in 0.125 seconds at 338.04KB/sec
```

```
...
```

```
...
```

```
Downloaded 606.85KB in 1.31 seconds at 463.24KB/sec
Downloaded 759.56KB in 1.607 seconds at 472.66KB/sec
Downloaded 865.73KB in 2.059 seconds at 420.46KB/sec
Downloaded 24.45KB in 0.109 seconds at 224.30KB/sec
Downloaded 474.03KB in 1.045 seconds at 453.61KB/sec
Downloaded 1.13MB in 2.387 seconds at 482.66KB/sec
Downloaded 448.57KB in 0.998 seconds at 449.47KB/sec
Downloaded 508.65KB in 1.17 seconds at 434.75KB/sec
Downloaded 3.63MB in 7.675 seconds at 484.29KB/sec
```

```
Downloaded 300 files/140.60MB in 283 seconds at 506.97KB/sec
```

NORMAN[®]

Client example code – multiple files per request

```
<?php
include('sampleshare.inc');

$share = new SampleShareObject();

$share->set_dates("2010-04-05 00:00:00","2010-04-06 00:00:00");
$share->set_http_user("<user>","<password>");
$share->set_url("sampleshare.norman.com/auth/sampleshare.php");
$share->set_max_blocksize("134217728");
$share->set_download_directory("d:/sampleshare/incoming");

$share->getlist();

foreach($share->md5list as &$entry) {
    /* Your code to determine if a sample should be downloaded here */
    if($download_this_sample==true) $entry["download"]=true;
}

$share->get_files_by_list();
echo "Downloaded $share->total_download_files samples/$share->total_download_size in $share->total_download_time
seconds at $share->total_download_avg_speed\r\n";

?>
```

Copyright © Normar AS

NORMAN**Client output – remote download with multiple files per request**

C:\PHP>php sampleshare.php

Requesting files shared between 2010-04-05 00:00:00 and 2010-04-06 00:00:00..

100 samples found. Starting download..

Downloading 100 files (62.44MB decrypted).. Ok!

Downloaded 72.96MB bytes in 119.388 seconds at 625.78KB/sec

Decrypting file with MD5 0FD216A2B4FBDB3F46C872D5F34F9FF4 - Filesize is 0000534266 bytes.. Done!

Decrypting file with MD5 7873C4FFEC9996E5F36E63F736FEB4F2 - Filesize is 0000021697 bytes.. Done!

Decrypting file with MD5 5FA6D328EFB6210D69ECAC90DF510F88 - Filesize is 0000042899 bytes.. Done!

Decrypting file with MD5 02D05E8C3BA83DD3D7394C6A63433E66 - Filesize is 0000043269 bytes.. Done!

...

...

Decrypting file with MD5 4ED4F0F6364DEFE75D0F3CB0D9DF1FA1 - Filesize is 0000485403 bytes.. Done!

Decrypting file with MD5 26CD4C92D8BEAE2959F54A760CFC90A9 - Filesize is 0001179769 bytes.. Done!

Decrypting file with MD5 6A7BF92358DDF23FDF8A2855FB824316 - Filesize is 0000459338 bytes.. Done!

Decrypting file with MD5 8DE5707AA8FA1D7A48CAA45311E3202A - Filesize is 0000520860 bytes.. Done!

Decrypting file with MD5 610FCA9992879FFBADAB8B6A334899BA - Filesize is 0003806167 bytes.. Done!

300 of 300 files downloaded

Downloaded 300 samples/140.60MB in 162 seconds at 888.76KB/sec

NORMAN[®]

Sample callback

```
<?  
...  
function myCallback($md5) {  
    global $share  
    /* Your code in here */  
}  
...  
$share->set_sample_callback("myCallback");  
...  
?>
```

Users can optionally specify a callback that will be called for each downloaded sample instead of waiting for the entire script to finish before sending samples to processing.

NORMAN[®]

Why stop there?

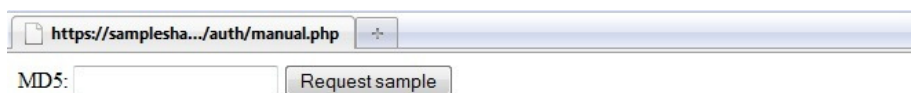
We can do more with this!



Copyright © Norman AGI

NORMAN[®]

Interface for manual sample requests



The screenshot shows a web browser window with the address bar containing the URL `https://samplesha.../auth/manual.php`. Below the address bar, there is a label "MD5:" followed by an empty text input field and a button labeled "Request sample".

Enables users to request single files of special interest

NORMAN[®]

Realtime sharing!

There is no longer any need to wait till the end of the month or week.

Samples can be shared as soon as you know they are malicious.



Copyright © Norman ASA

NORMAN[®]

Lets share cleanfiles!

```
<?
...
if($share->get_cleanfiles_list()) {
    foreach($share->md5list as &$entry) {
        // Your code to determine if a sample should be downloaded here
        if(<we want this file>) $entry["download"]=true;
    }
    $share->get_cleanfiles_by_list();
}
...
?>
```

The code is already there for you to use.

NORMAN

And of course – metadata!

```
<?
...
if($share->get_metadata()) {
    echo strlen($share->metadata)." bytes of metadata downloaded\r\n";
    /* Your metadata-parser here */
}
...
?>
```

Copyright © Norman AS

NORMAN®

Who is using it or who will?

- McAfee
- Sophos
- K7
- Andreas Marx

Who is next?

NORMAN[®]

To get a copy of our example framework, send mail me at trygve.brox@norman.com

Our server is already up and running, and you can start downloading samples from us using this framework today. If all goes well, we will stop sharing traditional samplepacks in a few months time.



NORMAN[®]



Any questions?

Copyright © Norman ASA