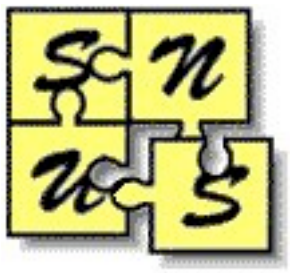
Öppna standarder, dokumentformat & Sender Policy Framework

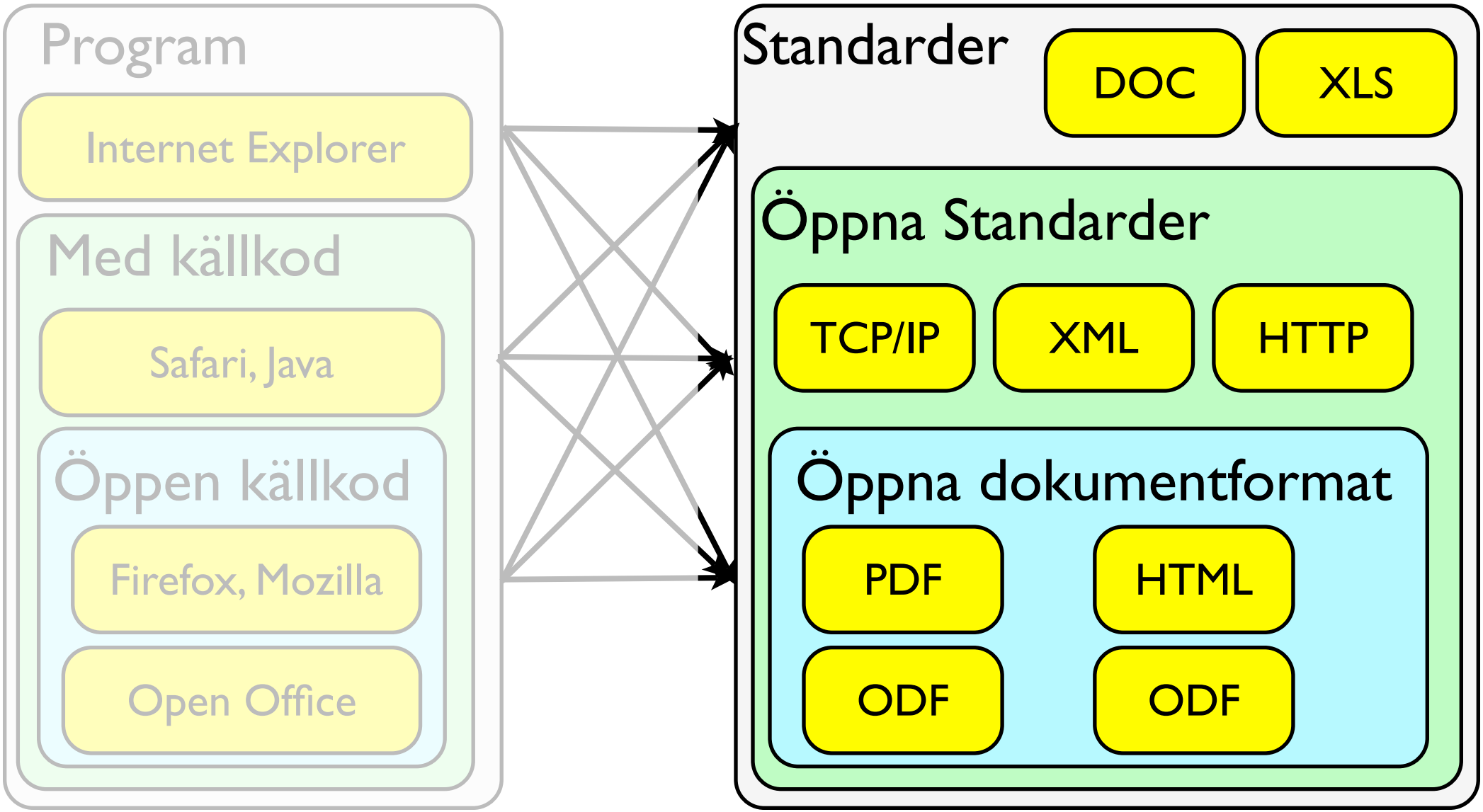
25 Maj 2007

Stefan Görling, stefan@gorling.se

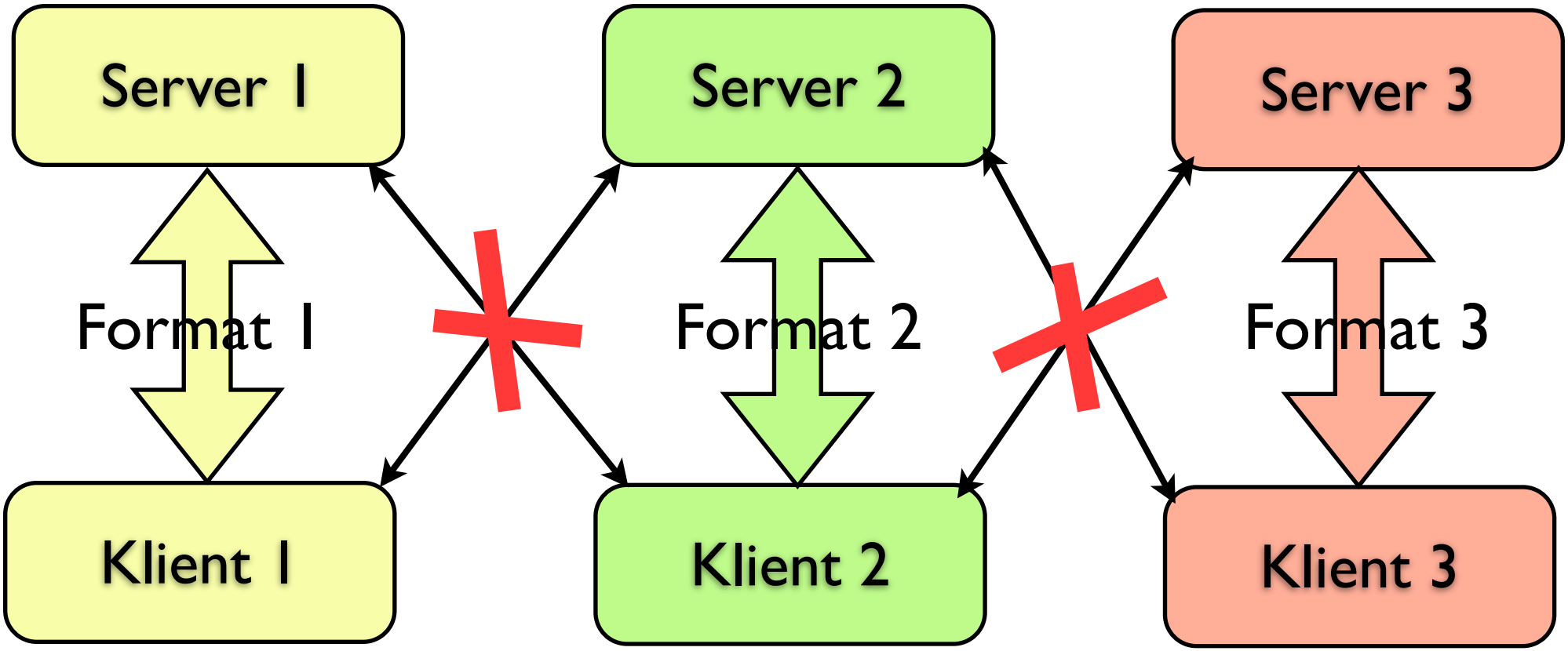


Del 1:
Öppna standarder & dokumentformat

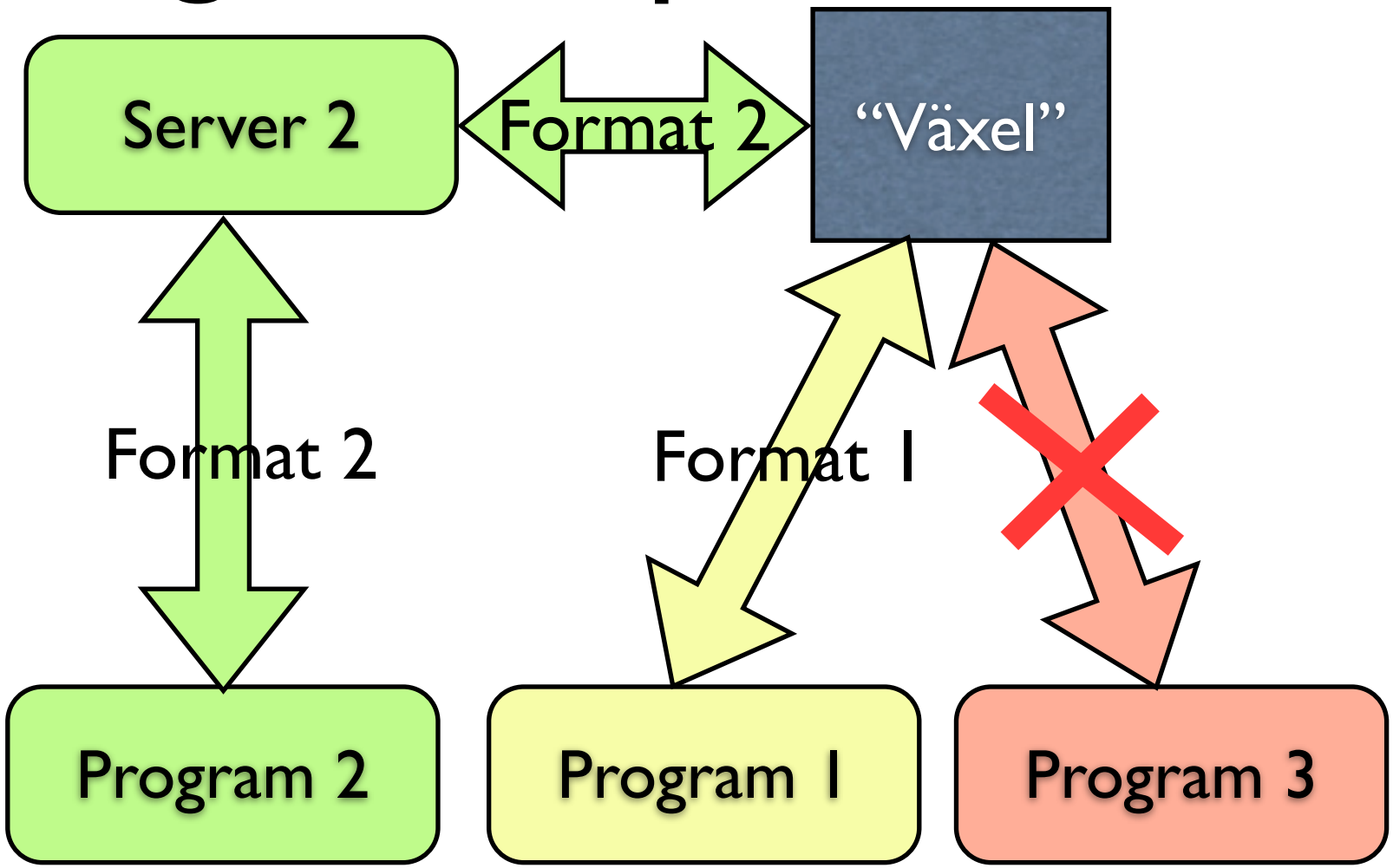
Standarder, dokument, (program)



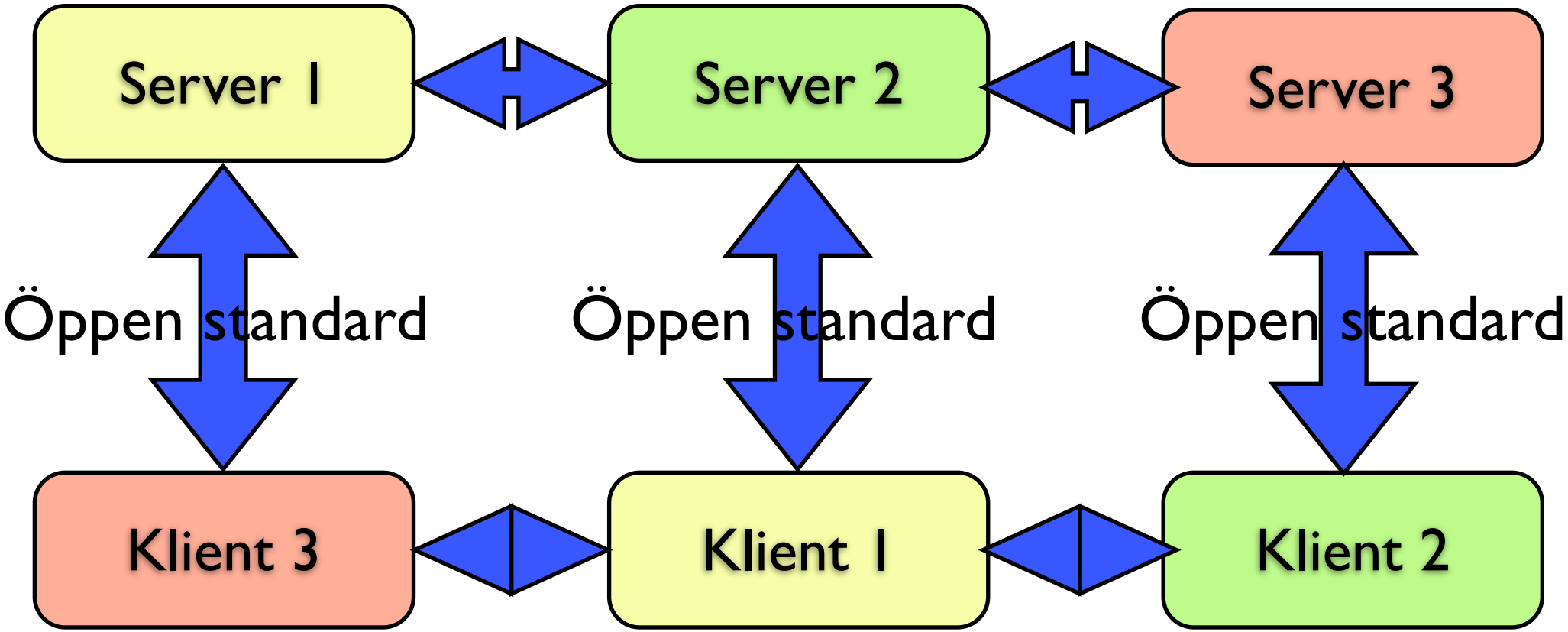
Slutna standarder



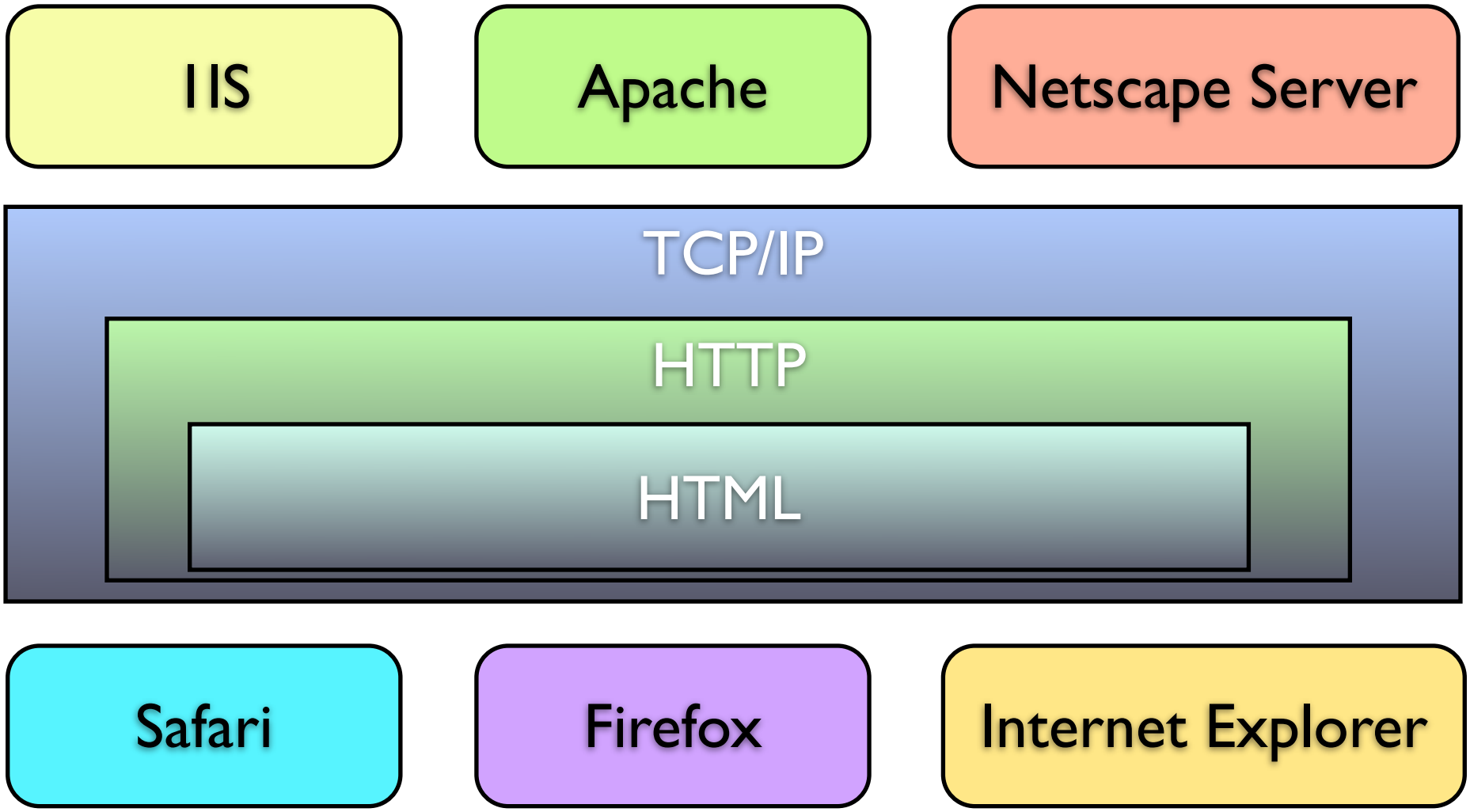
Integrationsproblem



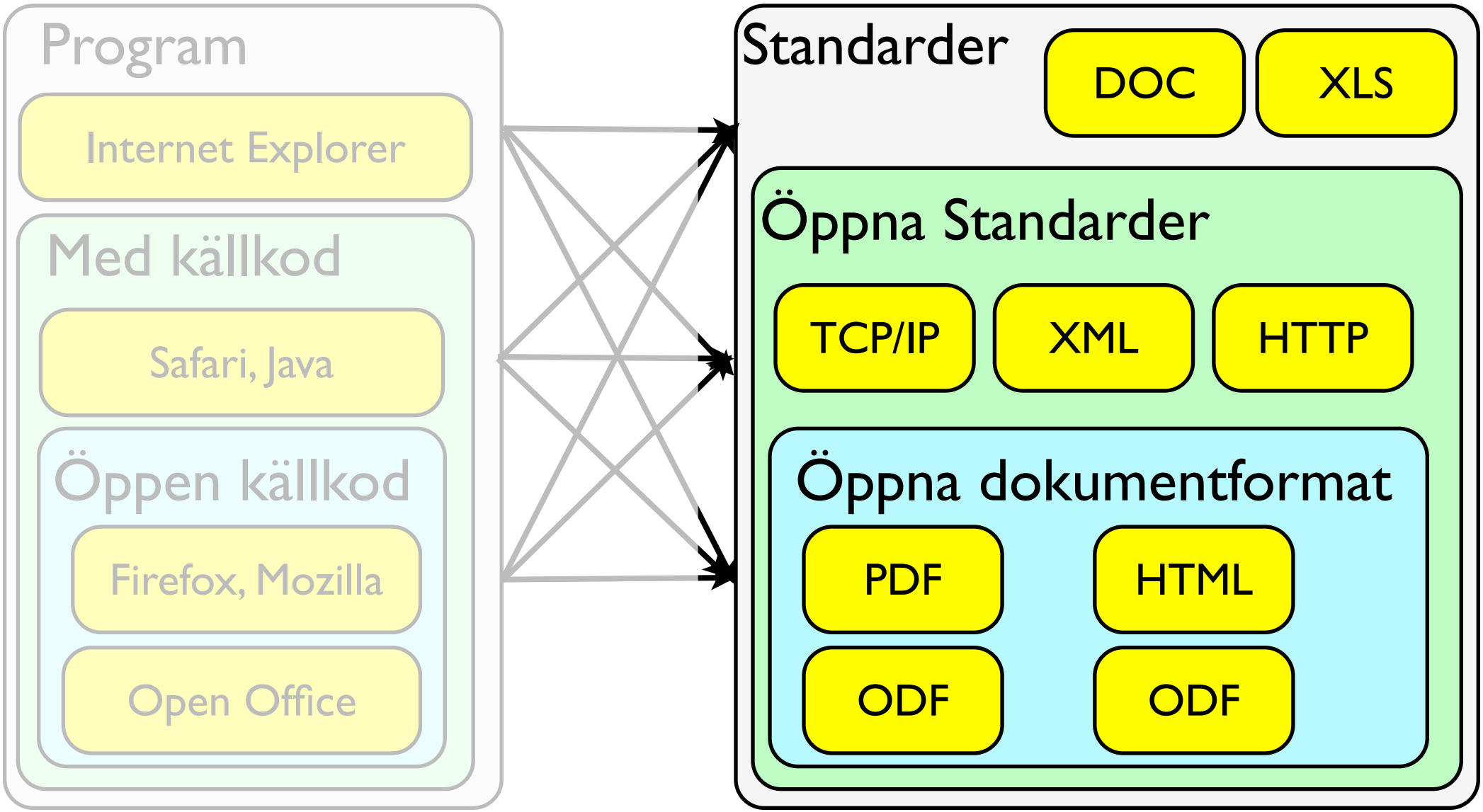
Öppna standarder



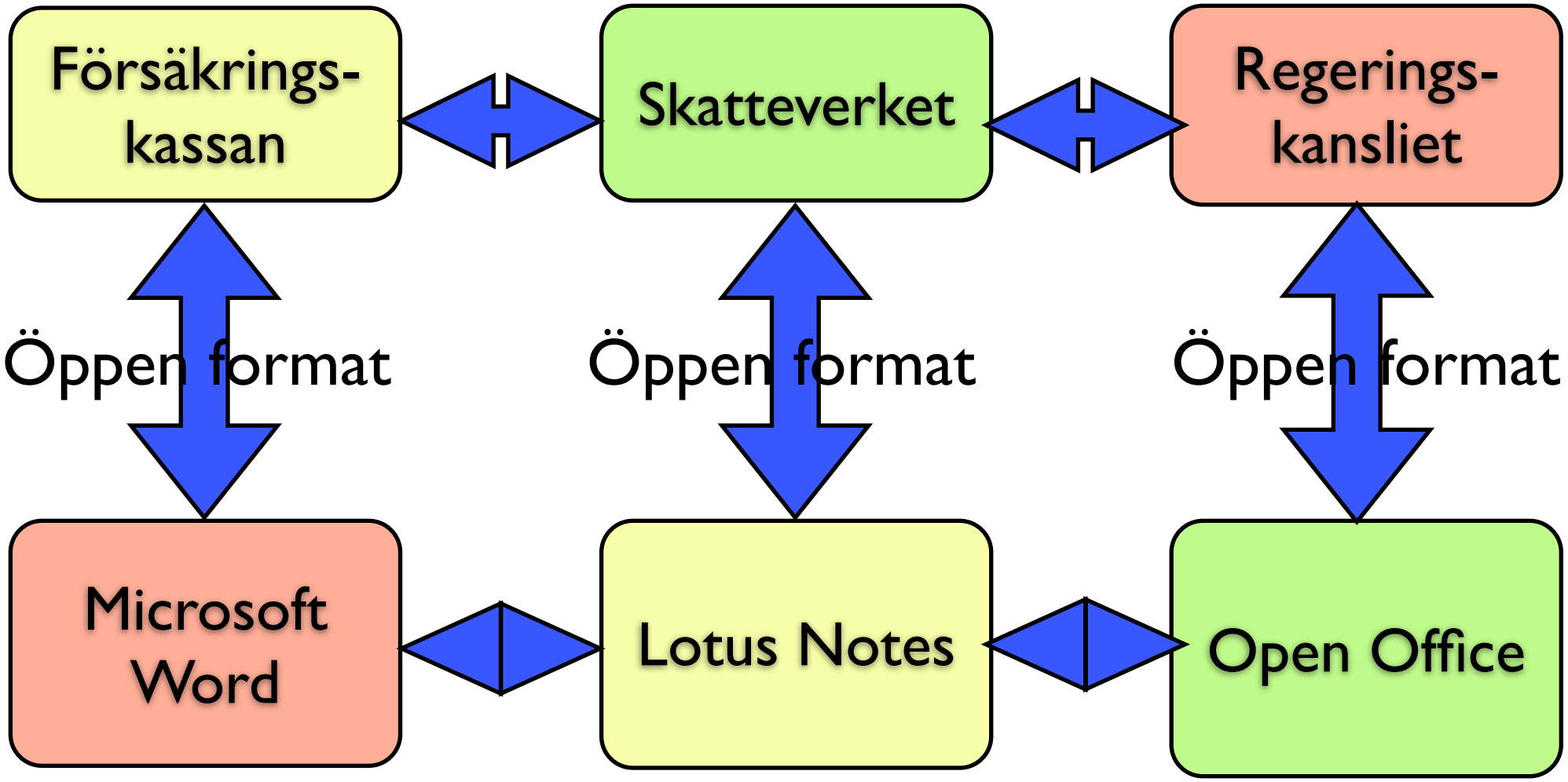
World Wide Web



Standarder, dokument, (program)



Öppna dokumentformat



Fördelar / Argument

- Undvika snedvridning av konkurrens och minskade inlåsningseffekter
- Förbättrad informationstillgång för medborgare
- Förenklat informationsutbyte mellan system
- Anpassningsmöjligheter till automatiserad handläggning
- Upphandling av funktion - ej applikation
- Minskade kostnader (på sikt)

Vad innebär öppenhet?

- Dokumenterat
- Standardiserat
- Demokratiskt
- Licensregler
- Icke-diskriminerande
- Innehållsneutralt
- Fullständigt
- Plattformsoberoende
- Spritt

Exempel på dokumentformat

Format	HTML	PDF	ODF	OOXML
Dokumenterat	Ja	Ja	Ja	Ja
Standardiserat	Ja, W3C	Delivs	Ja, ISO	Delvis, ECMA
Demokratiskt	Ja	Nej, Adobe	Ja, OASIS	Nej, Microsoft
Licensregler	Fritt	Idag royaltyfritt	Fritt	Idag royaltyfritt
Icke-diskriminerande	Ja	Ja, idag	Ja	Ja, idag
Innehållsneutralt	Ja	Ja, idag	Ja	Ja, idag
Fullständigt	Ja	Ja	Ja	Nej
Plattformsoberoende	Ja	Ja	Ja	Nej
Spritt	Ja, mycket	Ja, mycket	Ja	Nej
Öppet?	**Ja, definitivt**	**Ja, acceptabelt**	**Ja, definitivt**	**Nej**

Del 2:
Sender Policy Framework (SPF)

Spam - Kort översikt

- Har ändrat karaktär
- Mer spam, mindre som når oss
- Pump'n'Dump
- Maffiastrukturer
- Bildspam
- Phishing allt större problem

Angreppsätt

- Designa om SMTP
- Filtrering
- Öka transaktionskonstnaden
- Lagstiftning
- Blockera portar
- Avsändarautentisering

Avsändarautentisering

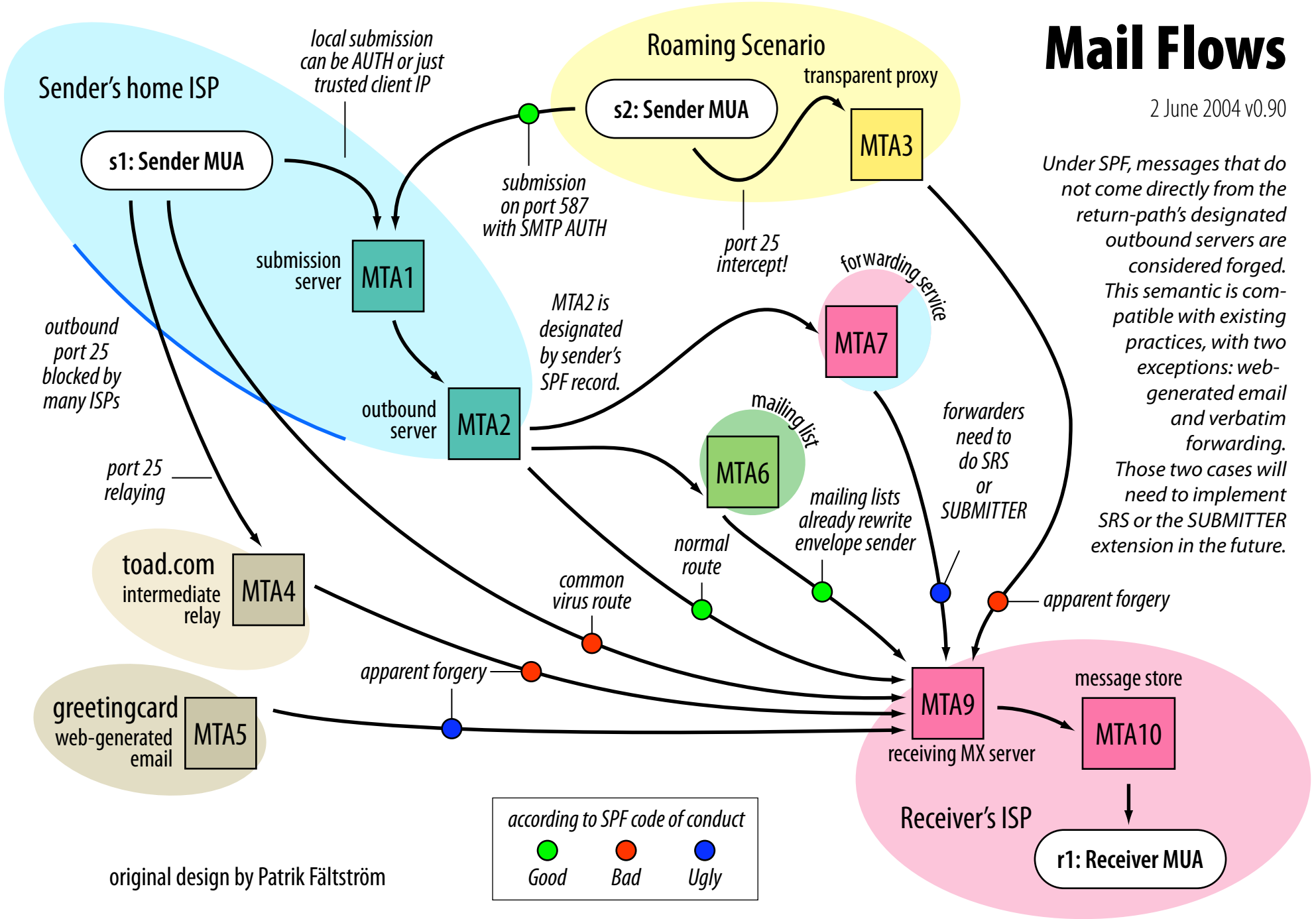
- Möjliggör verifikation av sändaren
- Minskar phishingproblematik
- Underlättar lokalisering av spammare

Standarder

Standard/ Mechanism	Transparent to user	Standardized	Authentication	Content verification	Public/ Private key-based	Protects from phishing
OpenPGP	No	Yes, since 1996	Yes, to individual	Yes	Yes	No
S/MIME	No	Yes, since 1998	Yes, to individual	Yes	Yes	No
SPF	Yes	Yes, experimental 2006	Yes, to domain	No	No	Yes
DomainKeys /DKIM	Yes	No, working on draft	Yes, to domain	Yes	Yes	No

Mail Flows

2 June 2004 v0.90



Under SPF, messages that do not come directly from the return-path's designated outbound servers are considered forged. This semantic is compatible with existing practices, with two exceptions: web-generated email and verbatim forwarding. Those two cases will need to implement SRS or the SUBMITTER extension in the future.

original design by Patrik Fältström

Glossary

DNSBL: an IP-based blacklist.
RHSBL: a domain-name blacklist, conceptually superior to DNSBLs, but less used today due to sender forgery. *(see SPF)*
SPF: an anti-forgery mechanism

Envelope sender *vs* header From

The envelope of an SMTP transaction is the stuff that comes before DATA. After DATA you get the message headers and body.

This is the envelope sender, also known as the return-path. SPF tests the domain of the envelope sender. If a message has a blank sender (MAIL FROM: <>), it could be a legitimate mailer-daemon bounce, or it could be a spam trying to look like one. Then SPF falls back to the hostname given in the HELO command.

This is the "From:" header. SPF does not look at the header "From:". Most mailing lists preserve the original "From:" address, but change the envelope sender to the special owner address which handles bounces. It would be wrong for SPF to examine this "From:" address. Besides, SPF's authorized sender mechanisms operate well before the header is transmitted, so this would come too late anyway.

Anatomy of an SMTP+SPF transaction

The moment an SPF-enabled MTA receives MAIL FROM, it can perform anti-forgery tests. If the tests fail, the MTA can assume the payload is probably a worm, virus, or spam without even looking at the payload DATA. If SPF tests pass, other tests (eg. RHSBLs) can be used with greater confidence. SPF makes the RHSBL a more powerful antispam tool.

at each SMTP stage...	... an SPF-enabled MTA can perform certain actions
connection to port 25	the MTA knows the client IP and thus the PTR name.
HELO *hostname*	if the *sender* (below) is empty, SPF uses *hostname* instead.
MAIL FROM: <*sender*>	SPF runs. If the transaction looks forged, an MTA can reject it right away, or prepend a header for later processing. If the transaction is not forged, the MTA should still perform other tests, such as RHSBLs.
RCPT TO: <*recipient*>	If all tests pass, the transaction proceeds.
DATA	Most domains that publish SPF use it to describe the hosts permitted to send mail from that domain, so forgeries can be rejected at MAIL phase. But some domains may prefer to use S/MIME, PGP/GPG, Habeas, or some other authentication mechanism which puts credentials in the headers or message body. Those domains still need to declare that messages without those credentials should be rejected. SPF supports such declarations also, even though they are less common. Some SPF-enabled MTAs prepend a Received-SPF header indicating the result, for later filters to use.
message header *Received-SPF: fail* *From: email@address*	
message body *Maybe there's PGP or S/MIME here. Parsing bodies is slow and costly.*	

Exempelpolicy

- bigbank.com: IN TXT “v=spf1 mx
- a:office.bigbank.com/28 -all"

Vanliga motargument

- Löser inte spamproblemet
- Anses inte vara tekniskt vacker - TXT records i DNS
- Kräver DNS-SEC för att vara helt säker
- Kräver att mail ska skickas från vissa servrar - anses vara fel
- Fungerar inte bra för automatisk forwarding

Fördelar

- Adresserar phishingproblematik
- Enkel att implementera
- Finns redan implementerat i de vanligaste spamfilterprogramvarornaFungerar, gör världen lite bättre
- Kanske inte lämpligt för alla organisationer, men mycket viktigt för många

Implementering i Sverige

- Hittills mycket lite intresse
- Nu inför storbankerna SPF
- Nästa steg är att få mailoperatörer att aktivera filtreringen.

Frågor / Diskussion

- Kontakt: stefan@gorling.se
- http://www.gorling.se/dokumentformat/
- http://www.gorling.se/spf/
- http://www.parasite-economy.com