

rxgk : GSSAPI based security for AFS

Simon Wilkinson

Introduction

- Why
- What
- How
- When
- How much?

Why?

Why?

DES

Why?

fcrypt

Why?

keyed
cache managers

Why?

cache poisoning

Why?

anonymous
cache managers

Why?

server enforced policy

Why?

departmental
file servers

Why?

secure callbacks

Why?

There's more to life
than Kerberos

What?

What?

rxgk

What?

GSSAPI based

What?

Plug in replacement
for existing security
layer

What?

Incremental
deployment

What?

confidentiality,
integrity protection

What?

authentication only

How?

How?

GSSAPI based key
negotiation

How?

Diffie Hellman based
key negotiation

How?

Token Combining Service

How?

New encryption layer

How?

Algorithm agility

(RFC3961 framework)

How?

Key versioning

When?

When?

Standardisation

When?

Implementation

When?

Integration

When?

Deployment

Questions

(and maybe some answers)