# TLS Origin-Bound Certificates

Wan-Teh Chang
IETF 82, 2011-11-17

# Introduction

Designers: D. Balfanz, D. Smetters, M. Upadhyay, and A. Barth, Google

Status: presented at IETF 81, Quebec City, implemented in NSS and OpenSSL

Goal: get this accepted as an official extension

# Stronger authentication for the web

Move away from **bearer tokens** (e.g., login cookies) on the web

Authenticate through **public key cryptography**

Short-term goal: keep cookies, but render cookie theft (e.g., through XSS) useless by binding cookies to the TLS channel

See www.browserauth.net for context

# Origin-Bound Certificates

Origin: the scheme://host:port part of a URL

Per-origin self-signed certificates

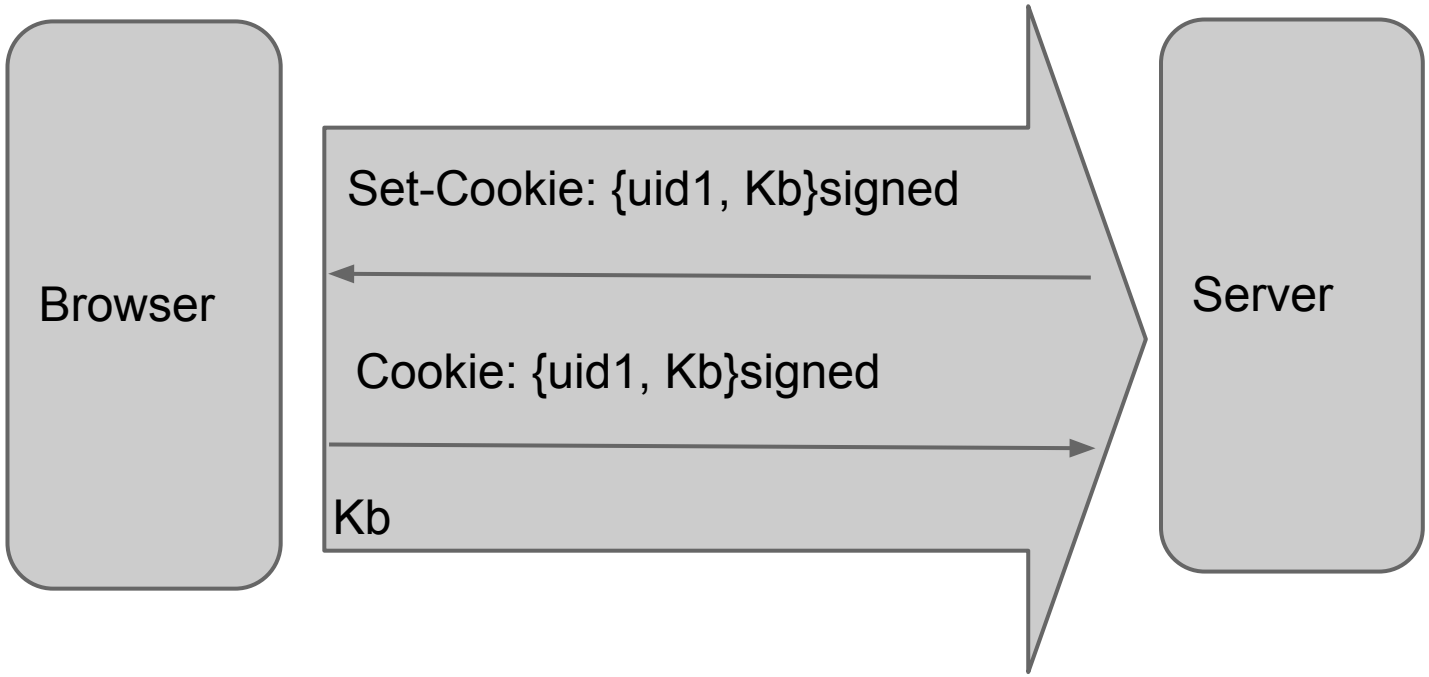
- generated on the fly on first visit
- used as TLS client-auth certificate

Servers bind login cookies to origin-bound certs

Browsers manage origin-bound certs like cookies

# Channel-Bound Cookies

Servers can bind cookies to client certificates



# TLS-OBC Extension

- ClientHello/ServerHello negotiate extension
- Server sends CertificateRequest
- Client ignores certificate_authorities in CertificateRequest (should be empty)
- Client generates origin-bound cert if necessary
- Client uses origin-bound cert in Client Auth
- Server accepts self-signed certs, ignores notBefore and notAfter
- Should be used with encrypted client certificates extension to protect client privacy

# Changes since -00 draft

Reviews of -00 draft on the TLS WG mailing list were generally positive

-01 draft: mostly editorial changes

- Use extension number 13175 for experiments
- Clarified how servers should use the web origin in the certificate extension
- Added key length recommendations in Security Considerations

# Implementation Status

Implemented in Chrome 17

Planning to run experiments on Google servers soon

Presented to Mozilla Firefox team for consideration and feedback