EDU DNSSEC Testbed

Shumon Huque, University of Pennsylvania
Larry Blunk, MERIT Network

Internet2 Joint Techs Conference
Salt Lake City, Utah
February 2nd 2010

DNSSEC

- “DNS Security Extensions”
- A system to verify the authenticity of DNS “data” using public key signatures
  - Protocol specs: RFC 4033, 4034, 4035, 5155

EDU Top Level Domain

- Operation of .EDU is managed by EDUCAUSE under a co-operative agreement with the US Dept of Commerce
- VeriSign is the current DNS operator for .EDU (the "registry")

Terminology

Registry	VeriSign Operator of EDU DNS zone
Registrar	EDUCAUSE Manages zone, registers entries
Registrant	EDU domain holders (upenn, berkeley, merit, etc ..)

Announcement

- September 3rd 2009

EDUCAUSE and VeriSign announced today the initiation of a project to enhance Internet reliability and stability. [.....]

The project will deploy a security system known as Domain Name Security Extensions (DNSSEC) within the .edu portion of the Internet, which EDUCAUSE manages under a cooperative agreement with the U.S. Department of Commerce. When the project is completed, institutions whose domain names end in .edu will be able to incorporate a digital signature into those names to limit a variety of security vulnerabilities.

Related change

- March 1st: VeriSign will be making modifications to .com/.net/.edu DNS servers specifically to support DNSSEC
- Involving referral and glue behavior
- https://lists.dns-oarc.net/pipermail/dns-operations/2010-January/004838.html

Feature summary

- NSEC3 with Opt-Out (RFC 5155)
- Signing algorithms
  - Testbed used 2048/1024 bit NSEC3 RSASHA1.
  - Production may use newer (RSASHA256 etc)?
- Any standardized DS hash algorithm supported (SHA-1, SHA-256, ...)
- DNSSEC function integrated into Educause’s web domain management application

DNSSEC Testbed

- Testbed planning discussion - March through August 2009
- Testbed operation: mid September through mid December 2009
- Multiple phases, gradually including more participants

DNSSEC FAQ

- (Answers to) Frequently Asked Questions
- http://net.educause.edu/edudnssecfaq

DNSSEC FAQ

- When will .edu be signed?
- Final deployment of DNSSEC for .edu will build on the previously announced US Dept of Commerce project to deploy DNSSEC at the authoritative root zone of the Internet. We anticipate .edu will be signed in the first half of 2010.

DNSSEC FAQ

- Do I have to do something with my domain?
- No. At launch, DNSSEC will be optional for .edu domain holders.

DNSSEC FAQ

- Will DNSSEC increase fees for .edu domain names?
- No. There will be no extra charges for .edu domain names.

Another doc

- Another recent publication by EDUCAUSE:
- “7 Things You Should Know About DNSSEC”
- http://www.educause.edu/library/EST1001
- Hard copies at JT Info Desk

7 Signed EDU subdomains (SLD)

berkeley.edu	University of California, Berkeley
merit.edu	MERIT Network
penn.edu	University of Pennsylvania
psc.edu	Pittsburgh Supercomputing Ctr
upenn.edu	University of Pennsylvania
internet2.edu	Internet2
ucaid.edu	Internet2

*** as of January 2010**

Looking further down ..

- SecSpider (http://secspider.cs.ucla.edu/) reports 58 more domains inside EDU
- Nearly half are 3rd level domains under Berkeley
- Quite a few are subdomains for CS, EECS, etc departments at universities (MIT, Kent State, Georgia Tech, RPI, Wisc) and DNS researchers (UCLA, Colorado State)

(as of January 2010)

Speaker change ..

DNSSEC Testbed

- Mid September through mid December 2009
- Test Registrar Tool (web application)
- Test EDU DNS server
- Participating EDU institutions:
  - Signed authoritative zones (test or production)
  - Validating resolvers

Participant phases

- 1. UPenn, UC Berkeley, MERIT
- 2. Harvard, Internet2, LSU, JHU, PSU
- 3. ARSC, CMU
- 4. Webster, Wichita State

What a DNSSEC signed delegation in EDU will look like ...

Cryptographically Secure Delegations are indicated by “DS” records and their signature (RRSIG).

```
      $ dig @x.x.x.x +norecurse +dnssec +multi www.merit.edu

      ;; QUESTION SECTION:
      ;www.merit.edu.                  IN      A

      ;; AUTHORITY SECTION:
      merit.edu.              86400 IN      NS      dns1.merit.net.
NS    merit.edu.              86400 IN      NS      dns2.merit.net.
      merit.edu.              86400 IN      NS      dns3.merit.net.
      merit.edu.              86400 IN DS 14556 5 1 (
                                      982113D08B4C6A1D9F6AEE1E2237AEF69F3F9759 )
DS    merit.edu.              86400 IN DS 14556 5 2 (
                                     F1E184C0E1D615D20EB3C223ACED3B03C773DD952D5F
                                      0EB5C777586DE18DA6B5 )
      merit.edu.              86400 IN RRSIG DS 7 2 86400 20100208154501 (
                                      20100125144501 4774 edu.
                                      KI33EqBmlCqLmQiLdLGbfFYtnI931lz2v9bsi2FFdvH
RRSIG                                 53lttgMKK3044ToH65xGCwDYS23xUDq1bwu0VLNGnAfl
  DS                                  V1GaIvEAAqVeMucfSE0sUzxgaNGtYyum2qMnQeo7bIgM
                                      UPizsh5ZImfyWw9If/LsWm7QToe6xcHZT5unnhc= )
```

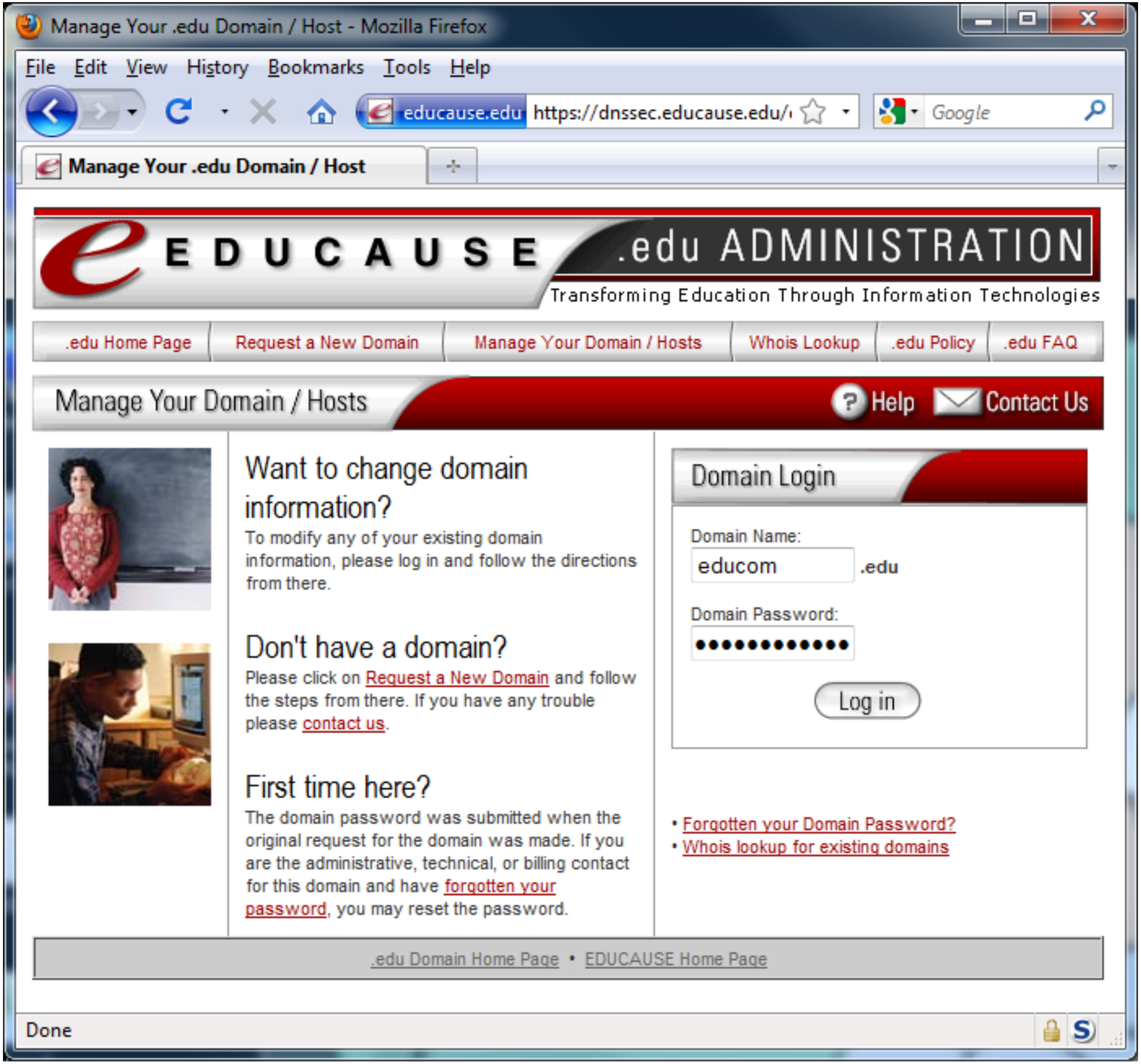
The parent DS record is a cryptographic hash of the entry point DNSKEY in the delegated zone

```
$ dig @198.108.1.43 merit.edu dnskey

;; QUESTION SECTION:
;merit.edu.             IN DNSKEY

;; ANSWER SECTION:
merit.edu.              7200 IN DNSKEY 257 3 7 (
                                AwEAAc6Z4l2Ne7mGyBWZDGegov2/LSJQgWOanV+UoTfe
                                AEWFGWa5yXKIKM9s+EeAHwORpGznNJIaGgxiOJ00H4IF
                                Cml6Z0tZeUvWadRzhtUKXEZqMtvuB+NM8WrrZs/1kSi2
                                jrf9jDctmPZDSHAjPhB4FQmeoLN+JJVbTZJ38iFHjdU+
                                hysTnIm4RYjAP/hLWXLeNLqtcbXwalu/ZTzXtt4lHVA/
                                C2/RqX1Xe/1VMe5/cYiW2bqLbUy9wUxiCVg6gOGBMVEO
                                JZwx/hcJG4n6CZXrdRJH0C8/EVg67DcW6BFfxfdLrLcd
                                WtnDxgYOC2noMP2U4CFiGmBNpTmgxVCuNx7Ct/M=
                                ) ; key id = 14556
```

[Note: only secure entry point DNSKEY shown]

Registration System

- Screenshots of the (planned) DNSSEC enabled registration system ..
- Slightly barebones. Final version will be enhanced with more helpful documentation and additional verbiage.


Manage Your .edu Domain / Host - Mozilla Firefox
File Edit View History Bookmarks Tools Help
educause.edu https://dnssec.educause.edu/
Google
Manage Your .edu Domain / Host
Done

EDUCAUSE .edu ADMINISTRATION

Transforming Education Through Information Technologies

.edu Home Page | Request a New Domain | Manage Your Domain / Hosts | Whois Lookup | .edu Policy | .edu FAQ

Manage Your Domain / Hosts

Help Contact Us

Want to change domain information?

To modify any of your existing domain information, please log in and follow the directions from there.

Don't have a domain?

Please click on Request a New Domain and follow the steps from there. If you have any trouble please contact us.

First time here?

The domain password was submitted when the original request for the domain was made. If you are the administrative, technical, or billing contact for this domain and have forgotten your password, you may reset the password.

Domain Login

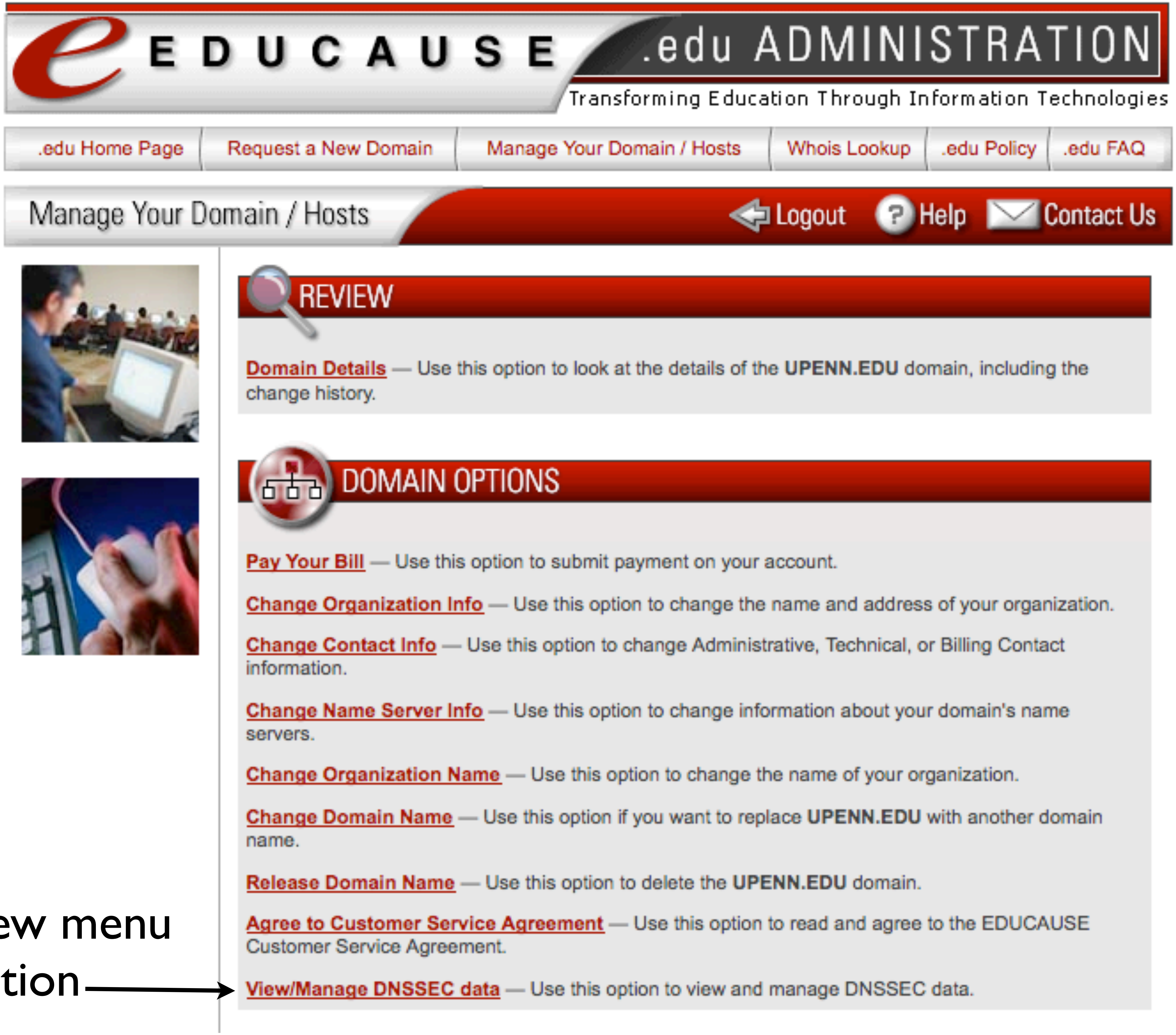
Domain Name: educom .edu

Domain Password: ●●●●●●●●●●●●

Log in

- Forgotten your Domain Password?
- Whois lookup for existing domains

.edu Domain Home Page • EDUCAUSE Home Page


EDUCAUSE .edu ADMINISTRATION
Transforming Education Through Information Technologies
.edu Home Page
Request a New Domain
Manage Your Domain / Hosts
Whois Lookup
.edu Policy
.edu FAQ
Manage Your Domain / Hosts
Logout
Help
Contact Us

REVIEW

Domain Details — Use this option to look at the details of the **UPENN.EDU** domain, including the change history.

DOMAIN OPTIONS

Pay Your Bill — Use this option to submit payment on your account.

Change Organization Info — Use this option to change the name and address of your organization.

Change Contact Info — Use this option to change Administrative, Technical, or Billing Contact information.

Change Name Server Info — Use this option to change information about your domain's name servers.

Change Organization Name — Use this option to change the name of your organization.

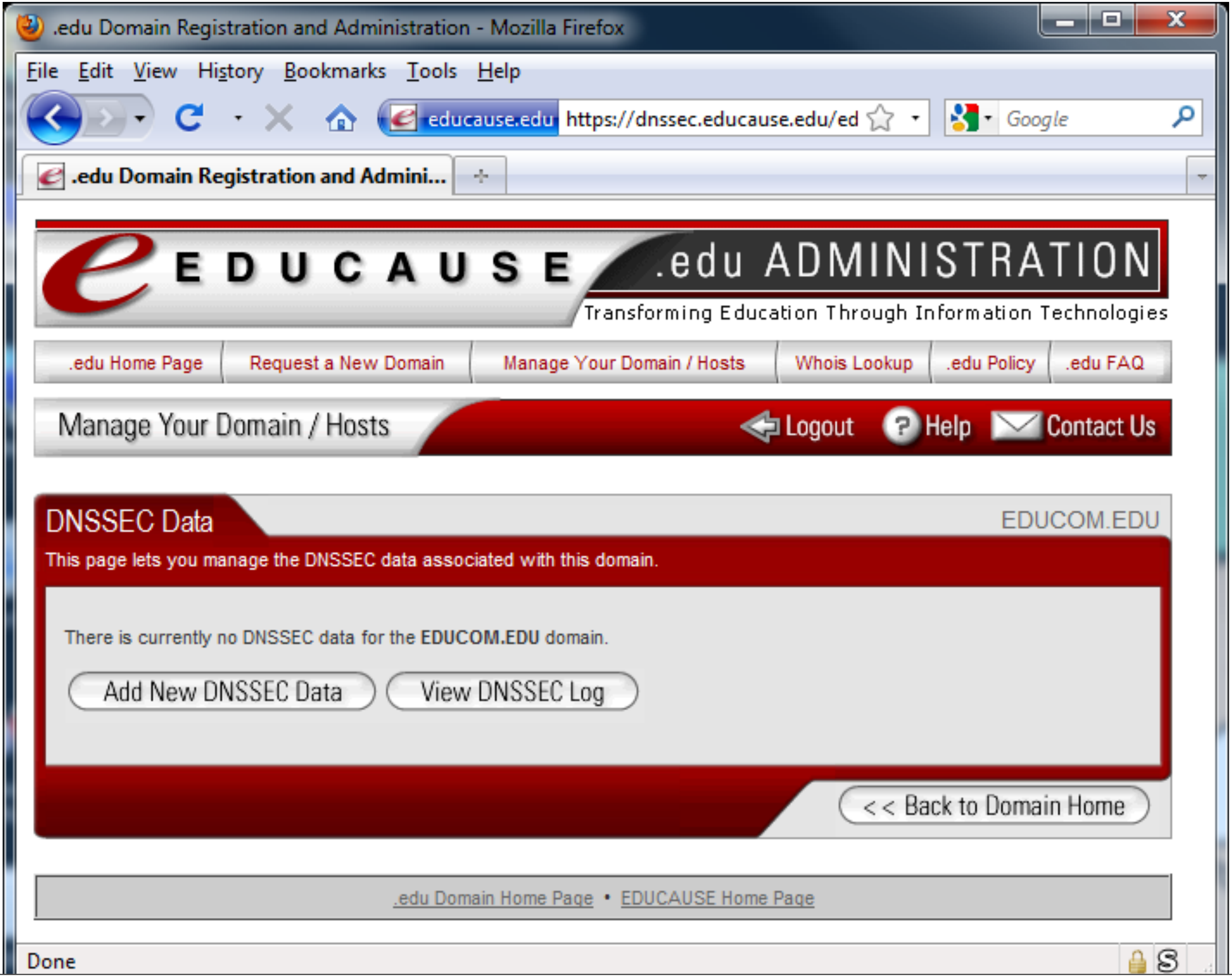
Change Domain Name — Use this option if you want to replace **UPENN.EDU** with another domain name.

Release Domain Name — Use this option to delete the **UPENN.EDU** domain.

Agree to Customer Service Agreement — Use this option to read and agree to the EDUCAUSE Customer Service Agreement.

View/Manage DNSSEC data — Use this option to view and manage DNSSEC data.

New menu option →


.edu Domain Registration and Administration - Mozilla Firefox
File Edit View History Bookmarks Tools Help
educause.edu https://dnssec.educause.edu/ed
Google
.edu Domain Registration and Admini...
EDUCAUSE .edu ADMINISTRATION
Transforming Education Through Information Technologies
.edu Home Page
Request a New Domain
Manage Your Domain / Hosts
Whois Lookup
.edu Policy
.edu FAQ
Manage Your Domain / Hosts
Logout
Help
Contact Us

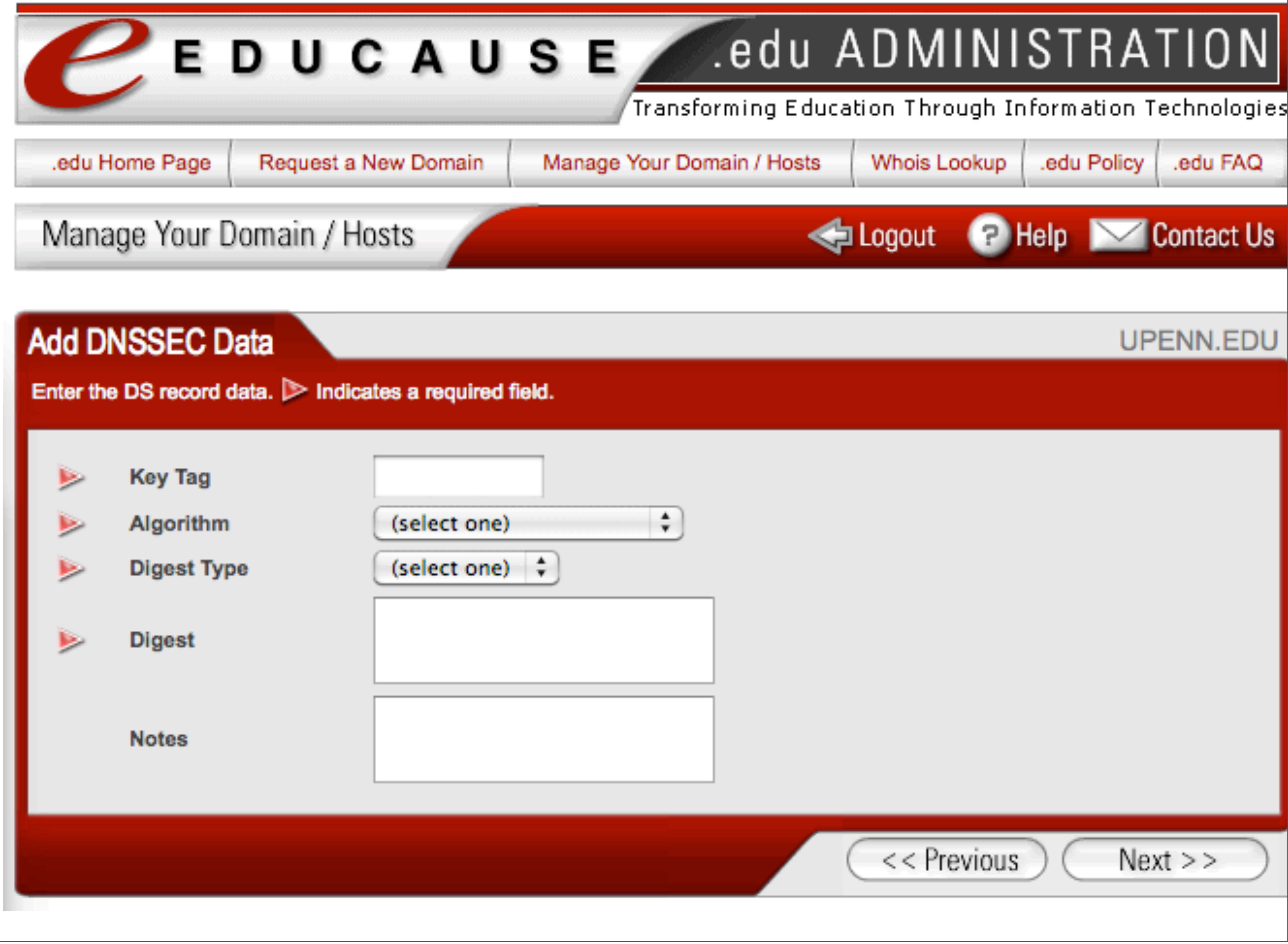
DNSSEC Data

EDUCOM.EDU

This page lets you manage the DNSSEC data associated with this domain.

There is currently no DNSSEC data for the **EDUCOM.EDU** domain.

Add New DNSSEC Data
View DNSSEC Log
<< Back to Domain Home
.edu Domain Home Page • EDUCAUSE Home Page
Done



Add DNSSEC Data

UPENN.EDU

Enter the DS record data. ▷ Indicates a required field.

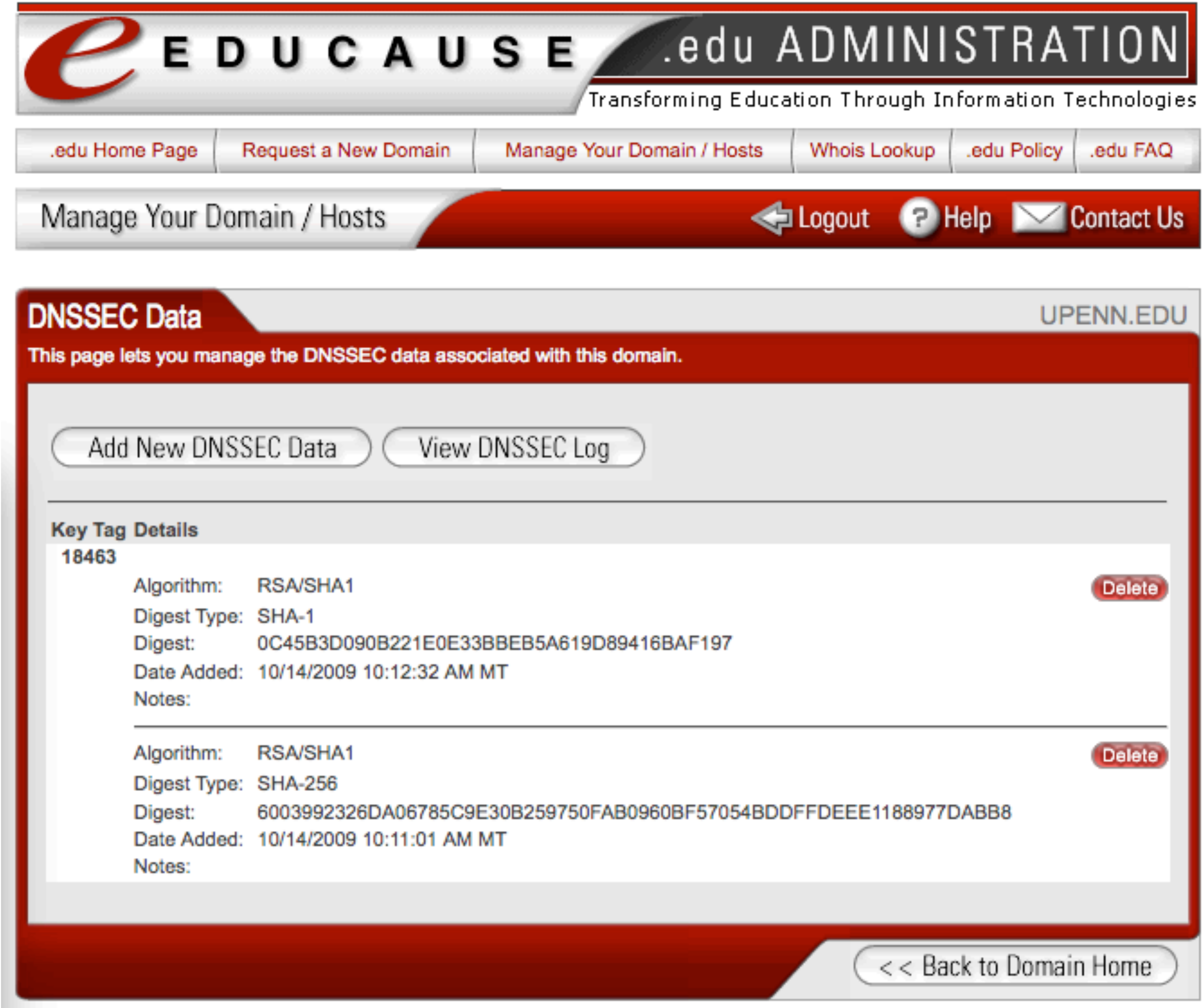
▷ Key Tag

▷ Algorithm (select one)

▷ Digest Type (select one)

▷ Digest

Notes



Manage Your Domain / Hosts

DNSSEC Data

UPENN.EDU

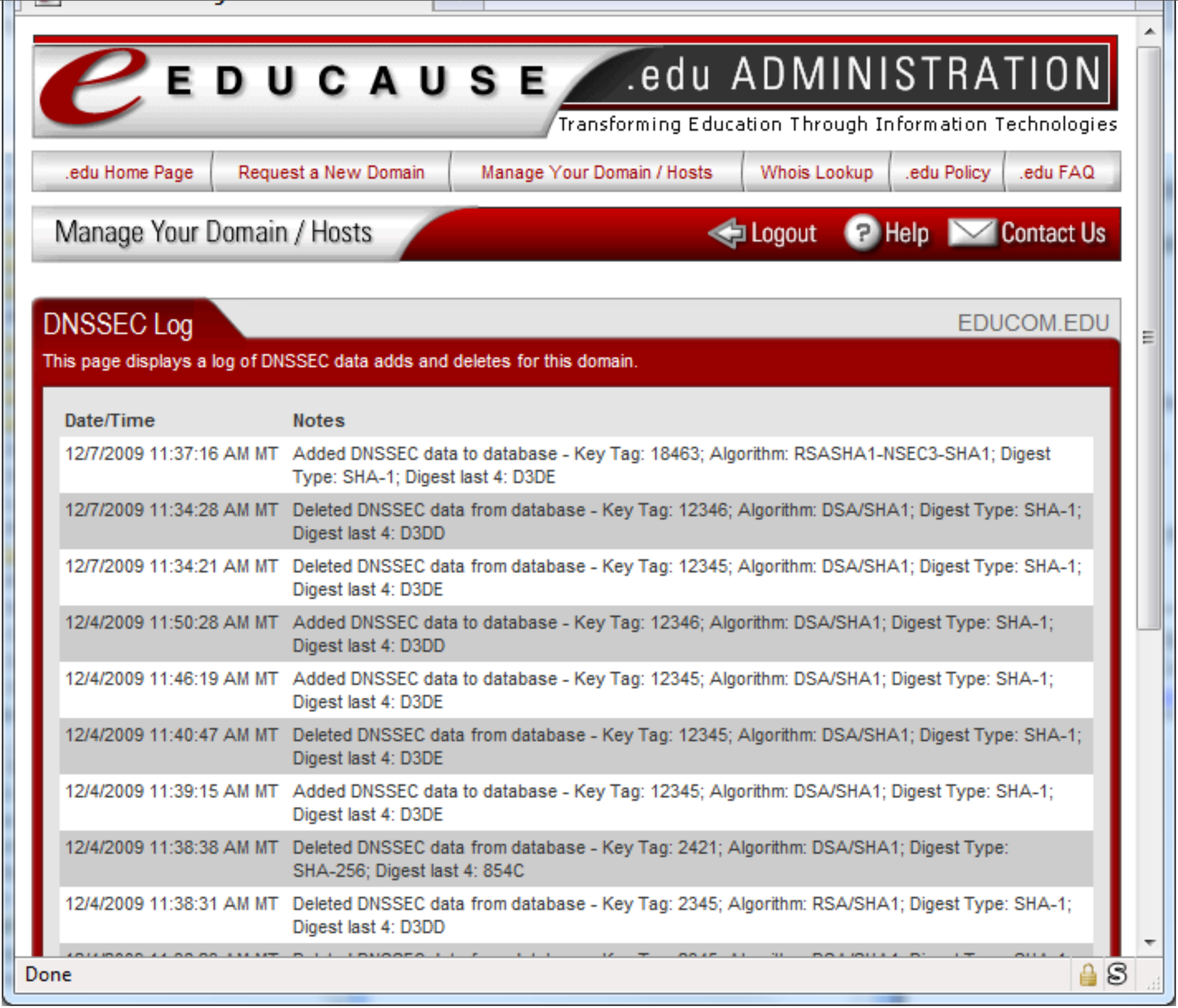
This page lets you manage the DNSSEC data associated with this domain.

Key Tag Details

18463

Algorithm:	RSA/SHA1
Digest Type:	SHA-1
Digest:	0C45B3D090B221E0E33BBEB5A619D89416BAF197
Date Added:	10/14/2009 10:12:32 AM MT
Notes:	

Algorithm:	RSA/SHA1
Digest Type:	SHA-256
Digest:	6003992326DA06785C9E30B259750FAB0960BF57054BDDFFDEEE1188977DABB8
Date Added:	10/14/2009 10:11:01 AM MT
Notes:	



Manage Your Domain / Hosts

DNSSEC Log

EDUCOM.EDU

This page displays a log of DNSSEC data adds and deletes for this domain.

Date/Time	Notes
12/7/2009 11:37:16 AM MT	Added DNSSEC data to database - Key Tag: 18463; Algorithm: RSASHA1-NSEC3-SHA1; Digest Type: SHA-1; Digest last 4: D3DE
12/7/2009 11:34:28 AM MT	Deleted DNSSEC data from database - Key Tag: 12346; Algorithm: DSA/SHA1; Digest Type: SHA-1; Digest last 4: D3DD
12/7/2009 11:34:21 AM MT	Deleted DNSSEC data from database - Key Tag: 12345; Algorithm: DSA/SHA1; Digest Type: SHA-1; Digest last 4: D3DE
12/4/2009 11:50:28 AM MT	Added DNSSEC data to database - Key Tag: 12346; Algorithm: DSA/SHA1; Digest Type: SHA-1; Digest last 4: D3DD
12/4/2009 11:46:19 AM MT	Added DNSSEC data to database - Key Tag: 12345; Algorithm: DSA/SHA1; Digest Type: SHA-1; Digest last 4: D3DD
12/4/2009 11:40:47 AM MT	Deleted DNSSEC data from database - Key Tag: 12345; Algorithm: DSA/SHA1; Digest Type: SHA-1; Digest last 4: D3DE
12/4/2009 11:39:15 AM MT	Added DNSSEC data to database - Key Tag: 12345; Algorithm: DSA/SHA1; Digest Type: SHA-1; Digest last 4: D3DE
12/4/2009 11:38:38 AM MT	Deleted DNSSEC data from database - Key Tag: 2421; Algorithm: DSA/SHA1; Digest Type: SHA-256; Digest last 4: 854C
12/4/2009 11:38:31 AM MT	Deleted DNSSEC data from database - Key Tag: 2345; Algorithm: RSA/SHA1; Digest Type: SHA-1; Digest last 4: D3DD

Participant requirements

- Authoritative DNS servers running signed zones (test servers ok)
- Validating resolvers, configured to use EDU testbed servers as authority (eg. via the “stub zone” feature in BIND, Unbound)

Overview of Tests

- [set of tests of the EPP interface between registrar & registry]
- This is between Educause and Verisign, so not that interesting for EDU domain holders

Overview of Tests

- confirm connectivity to testbed
- Add DS records of various algorithms & digest types
- Add additional DS record(s)
- Remove DS record(s)
- Add incorrect DS record(s)
- View DS record history report
- Perform key rollover operations and DS updates

Overview of Tests

- At each test stage perform verification tests with an appropriately configured validating resolver
  - edu trust anchor
  - stub zone for edu pointing to testbed servers
- Attempt to validate records in the zones of other participants also

Summary Results

- For the most part, everything worked as expected
- A few small bugs were fixed
- A few accidental key expirations and incorrect participant zone signings happened (hey, it's a testbed!)
- Support for registering multiple DS records was added
- Debate about submitting DNSKEY vs DS records to registrar

References

- http://net.educause.edu/edudnssecfaq
- http://www.educause.edu/library/EST1001
- https://www.dnssec-deployment.org/index.php/deployment-case-studies/internet-2/

Questions/Comments?

- Shumon Huque, shuque [at] upenn.edu
- Larry Blunk, ljb [at] merit.edu